CENTRAL SITE REMOTE ACCESS SWITCH USER'S GUIDE

Release 7.4

Cabletron Systems

(603) 332-9400 phone
(603) 337-3075 fax
support@ctron.com

Only qualified personnel should perform installation procedures.

NOTICE

You may post this document on a network server for public use as long as no modifications are made to the document.

Cabletron Systems reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Cabletron Systems to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL CABLETRON SYSTEMS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

Cabletron Systems, Inc.
P.O. Box 5005
Rochester, NH 03866-5005

Order Number: 9032186-04

VIRUS DISCLAIMER

Cabletron Systems has tested its software with current virus checking technologies. However, because no anti-virus system is 100% reliable, we strongly caution you to write protect and then verify that the Licensed Software, prior to installing it, is virus-free with an anti-virus system in which you have confidence.

Cabletron Systems makes no representations or warranties to the effect that the Licensed Software is virus-free.

TRADEMARKS

Cabletron Systems, CyberSWITCH, MMAC-Plus, SmartSWITCH, SPECTRUM, and SecureFast Virtual Remote Access Manager are trademarks of Cabletron Systems, Inc.

All other product names mentioned in this manual are trademarks or registered trademarks of their respective companies.

COPYRIGHTS

All of the code for this product is copyrighted by Cabletron Systems, Inc.

Portions of the code for this product are copyrighted by the following corporations:

FCC NOTICE

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment uses, generates, and can radiate radio frequency energy and if not installed in accordance with the operator's manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference in which case the user will be required to correct the interference at his own expense.

WARNING: Changes or modifications made to this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

DOC NOTICE

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

VCCI NOTICE

This is a Class 1 product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は、第一種情報装置（商工業地域において使用されるべき情報装置）で商工業地域での電波障害防止を目的とした情報処理装置等電波障害自主規制協議会（VCCI）基準に適合しております。
従って、住宅地域またはその隣接した地域で使用すると、ラジオ、テレビジョン受信機等に受信障害を与えることがあります。
取扱説明書に従って正しい取り扱いをして下さい。

CABLETRON SYSTEMS, INC. PROGRAM LICENSE AGREEMENT

IMPORTANT: Before utilizing this product, carefully read this License Agreement.

This document is an agreement between you, the end user, and Cabletron Systems, Inc. ("Cabletron") that sets forth your rights and obligations with respect to the Cabletron software program (the "Program") contained in this package. The Program may be contained in firmware, chips or other media. BY UTILIZING THE ENCLOSED PRODUCT, YOU ARE AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE UNUSED PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.

CONTENTS

USING THIS GUIDE 25

Documentation Set 26
Guide Conventions 27

SYSTEM OVERVIEW 29

The CyberSWITCH 30

Unique System Features 31
Interoperability Overview 34
Interoperability Protocols 34
Interoperability Devices 35
Encryption Overview 36
Network Layer 36
Link Layer 36
Security Overview 37
Network Interface Overview 37
System Components 38
Remote ISDN Devices 39
Switches Supported 40

Hardware Overview 41

System Platforms 41
The CSX5500 42
Platform Description 42
Cleaning the CSX5500 Air Filter 43
Platform Characteristics 44
Caution for DC-Powered CSX5500s 45
The CSX6000 46
Platform Description 46
Cleaning the CSX6000 Air Filter 47
Platform Characteristics 47
Caution for DC-Powered CSX6000s 48
The CSX7000 49
Platform Description 49
Platform Characteristics 49
Caution for DC-Powered CSX7000s 50
The NE 2000-II (A Network Express Platform) 51
Platform Description 51
Platform Characteristics 52
The NE 4000 (A Network Express Platform) 53
Platform Description 53
Platform Characteristics 53
The NE 5000 Platform (A Network Express Platform) 55
Platform Description 55
Cleaning the NE 5000 Air Filter 56
Platform Characteristics 57

System Adapters 58
Ethernet Adapters 58
Ethernet-2 Adapter 58
Ethernet-1 Adapter 58
Hardware Characteristics 59
LAN Connection 59
Basic Rate Adapters 59
BRI-4 Basic Rate Adapter 59
BRI-1 Basic Rate Adapter 60
BRI Connection 60
Primary Rate Adapters 61
The PRI-8 61
The PRI-23 61
The PRI-23/30 62
PRI-8, PRI-23, and PRI-23/30 Connection 63
Expander Adapter 63
Hardware Characteristics 63
V.35 Adapter 64
Hardware Characteristics 64
V.35 Connection 64
RS232 Adapter 65
Hardware Characteristics 66
RS232 Connection 66
Digital Modems 67
The DM-8 68
The DM-24 68
The DM-24+and DM-30+ 68
Encryption Adapter 69

Software Overview 70
System software 70
Administration software 70
System Files 71
Configuration Files 71
Operational Files 72
User Level Security Files 73

SYSTEM INSTALLATION 74

Ordering ISDN Service (US Only) 75
Overview 75
Ordering NI-1 Lines Using EZ-ISDN Codes 75
Ordering NI-1 Lines Using NI-1 ISDN Ordering Codes 75
Ordering BRI ISDN Lines using Provisioning Settings 75
Provisioning Settings for AT&T 5ESS Switches 76
AT&T 5ESS NI-1 Service 77
AT&T 5ESS Custom Point-to-Point Service 78
Provision Settings for Northern Telecom DMS-100 Switches 78
Northern Telecom DMS100 NI-1 Service 79
Northern Telecom DMS100 Custom Service 80
Basic Information for Ordering PRI ISDN Lines 80

Hardware Installation 83
Overview 83
Pre-Installation Requirements 83
Selecting Slots for the Adapters 84
Adapter Settings 85
Adapter Interrupt and I/O Address Settings 86
WAN Adapters 86
DM-8 Adapter I/O Address Settings 86
DM-24 Adapter Interrupt and I/O Address Settings 87
DM-24+ and the DM-30+ Adapter Address Settings 88
Encryption Adapter Settings 89
MVIP Settings 89
Additional Adapter Settings 90
PRI-8 90
PRI-23 91
PRI-23/30 92
Inserting the Adapters into the CyberSWITCH 93
Connecting Adapter Inter-Board Cables 94
Connecting Multiple Adapters 94
Connecting a WAN Adapter to the LCD 96
Summary of Guidelines 97
Cabling Guidelines 97
Termination Guidelines 97

Accessing the CyberSWITCH 98
Overview 98
Making Connections 98
Direct Connection 98
Null-Modem Connection to a PC 99
Remote Connection using Telnet 100
Remote Connections (Modem to Modem) 101
Analog Modem on the CyberSWITCH 101
Digital Modem on the CyberSWITCH 102
Establishing an Administration Session 103
Accessing the Release Notes 104

Upgrading System Software 105
Overview 105
Installing Software 105
Upgrading System Software 107
Local Upgrade 107
Procedure 107
Handling Upgrade Warnings and Errors 108
Remote Upgrade 108
Accessing the Release Notes 109

BASIC CONFIGURATION 110

Configuration Tools 111

- Overview 111
- CFGEDIT 111
  - Executing CFGEDIT 112
  - Saving CFGEDIT Changes 112
- Dynamic Management 112
  - Executing Dynamic Management 112
  - Utility Dynamic Management Commands 113
  - Saving Dynamic Management Changes 113
- Using the Network Worksheets 114
- Using the Configuration Chapters 114

Configuring Resources and Lines 115

- Overview 115
- Resources 115
  - Configuring Resources 115
  - Resource Configuration Elements 116
  - Resource Background Information 117
- Lines 119
  - Configuring Lines 119
    - Configuring a Line for a BRI Resource 119
    - Configuring a Line for a PRI Resource 119
    - Configuring a Line for V.35 and RS232 Resources 120
    - Configuring Changes for a COMMPORT Resource 121
  - Line Configuration Elements 122
  - Line Background Information 126
    - R2 Signaling 127
- Subaddresses 127
  - Configuring a Subaddress 127
  - Subaddress Configuration Elements 127
  - Subaddresses Background Information 127

Configuring Basic Bridging 128

- Overview 128
- MAC Layer Bridging Option 128
  - Enabling / Disabling Bridging 128
  - MAC Layer Bridging Configuration Elements 128
  - MAC Layer Bridging Background Information 129

Configuring Basic IP Routing 130

- Overview 130
- Internet Protocol (IP) Option 130
  - Enabling IP 130
  - IP Option Configuration Elements 131
  - IP Background Information 131
- IP Operating Mode 131
  - Configuring the IP Operating Mode 131
  - IP Operating Mode Configuration Elements 132
  - IP Operating Mode Background Information 132

IP Network Interfaces 133
Configuring Interfaces 133
Network Interface Configuration Elements 135
IP Network Interface Background Information 140
IP RIP and the IP Network Interfaces 145
IP RIP over Dedicated Connections 148
IP Host Operating Mode and the IP Network Interfaces 150
Using Multiple IP Addresses 150
Static Routes 152
Configuring Static Routes 152
Static Route Configuration Elements 154
Static Route Background Information 156
Default Routes 157
Configuring Default Routes 157
Default Route Configuration Elements 157
Routing Information Protocol (RIP) Option 158
Enabling / Disabling IP RIP 158
IP RIP Configuration Elements 159
IP RIP Background Information 159

SECURITY AND ENCRYPTION OPTIONS 160

Security Overview 161
Overview 161
Security Level 161
System Options and Information 162
Device Level Databases 162
User Level Databases 163
Off-node Server Information 163
Network Login Information 163

Configuring Security Level 164
Overview 164
No Security 166
Configuring No Security 166
Device Level Security 167
Configuring Device Level Security 167
Device Level Security Background Information 167
Overview of Device Authentication Process 168
User Level Security 168
Configuring User Level Security 168
User Level Security Background Information 168
Authentication Using a Security Token Card 169
System Requirements 170
Authentication Process with User Level Security 171
Device and User Level Security 172
Configuring Device and User Level Security 172
Device and User Level Background Information 173

Configuring System Options and Information 174

- Overview 174
- System Options 174
  - Configuring System Options 174
  - System Options Configuration Elements 175
  - System Options Background Information 177
- System Information 178
  - Configuring System Information 178
  - System Information Configuration Elements 178
  - System Information Background Information 179
- Administrative Session 179
  - Configuring Administrative Sessions 179
  - Administrative Session Configuration Elements 180
  - Administrative Session Background Information 181
    - Alternative Database Location Background Information 181
    - Session Inactivity Background Information 181
    - Number of Administrative Telnet Sessions Background Information 181
    - Telnet Server TCP Port Number Background Information 181
    - Emergency Telnet Server Port Number Background Information 182

Configuring Device Level Databases 183

- Overview 183
- On-node Device Database 183
  - Configuring an On-node Device Database 183
- On-node Device Entries 184
  - Configuring On-node Device Entries 184
  - On-node Device Database Configuration Elements 191
    - General Configuration Elements 191
    - ISDN Configuration Elements 191
    - Frame Relay Access Configuration Elements 193
    - X.25 Access Configuration Elements 193
    - Digital Modem Configuration Elements 194
    - Authentication Configuration Elements 194
    - IP Information Configuration Elements 196
    - IPX Information Configuration Elements 196
    - AppleTalk Information Configuration Elements 197
    - Bridge Information Configuration Elements 198
    - Compression Configuration Elements 199
  - On-node Device Database Background Information 199
    - On-node Device Database Security Requirements 199
- Off-node Device Database Location 203
  - Configuring Off-node Device Database Location 203
  - Off-node Device Database Location Configuration Elements 204
  - Off-node Device Database Location Background Information 204

Configuring User Level Databases 205

- Overview 205
- User Level Authentication Database Location 205
  - Configuring Authentication Database Location 205
  - User Level Authentication Database Location Configuration Elements 206
  - User Level Authentication Database Location Background Information 206

Configuring Off-node Server Information 207

Overview 207
Multiple Administration Login Names 207
CSM Authentication Server 208
Configuring CSM Authentication Server 208
CSM Authentication Server Configuration Elements 209
CSM Authentication Server Background Information 209
RADIUS Server 209
Configuring a RADIUS Authentication Server 209
RADIUS Authentication Server Configuration Elements 211
RADIUS Authentication Server Background Information 211
Configuring a RADIUS Accounting Server 212
RADIUS Accounting Server Configuration Elements 214
RADIUS Accounting Server Background Information 214
Performance 214
Verification and Diagnosis 215
RADIUS RFC2138 215
Enabling RADIUS Type 215
RADIUS Type Configuration Elements 216
Background Information 216
Dynamic Device Option 216
Configuring the Dynamic Device Option 216
Dynamic Device Configuration Elements 217
Background Information 217
TACACS Authentication Server 218
Configuring a TACACS Authentication Server 218
TACACS Authentication Server Configuration Elements 219
TACACS Authentication Server Background Information 219
ACE Authentication Server 220
Configuring an ACE Authentication Server 220
Alternate Method of Configuration 221
ACE Authentication Server Configuration Elements 221
ACE Authentication Server Background Information 222

Configuring Network Login Information 223

Overview 223
Network Login General Configuration 223
Configuring General Network Login Information 223
Authentication Timeout 224
Terminal Server Security 224
Network Login General Configuration Background Information 225
Network Login Banners 225
Configuring Network Login Banners 225
Network Login Banners Background Information 226
Login Configuration Specific to RADIUS Server 226
Configuring RADIUS Server Login Information 226
Login Configuration Specific to RADIUS Server Background Information 227
Login Configuration Specific to TACACS Server 228
Configuring TACACS Server Login Information 228
Login Configuration Specific to TACACS Server Background Information 229

Configuring Encryption 231

Configuration 231
- Configuring an Encryption adapter 231
- Configuring Security Associations and Authentication (IP Security Only) 232
- Configuring Link Layer Encryption (PPP Encryption Only) 233
- Encryption Configuration Elements 234

Encryption Background Information 236
- IP Network Layer Encryption 236
  - ESP Implementation 236
  - IP Encryption Example 237
  - Authentication Headers 237
- Link Layer Encryption 238
  - Link Layer Encryption: Manually-Configured Keys 238
  - Automated Key Exchange 239
- Interaction with Other Features 239
  - IP Filters 239
  - Multiple MAC/IP Addresses 240
  - PPP Compression 240

ADVANCED CONFIGURATION 241

Configuring Alternate Accesses 242

Overview 242

Dedicated Accesses 242
- Configuring a Dedicated Access 242
- Dedicated Access Configuration Elements 243
- Dedicated Access Background Information 243

X.25 Accesses 244
- Configuring an X.25 Access 244
  - Basic Configuration Information 244
  - LAPB Configuration Information 245
  - X.25 Configuration Information 245
  - Permanent Virtual Circuit Information 247
- X.25 Configuration Elements 247
  - X.25 Line Configuration Elements 247
  - LAPB Configuration Elements 248
  - X.25 Access Configuration Elements 249
  - PVC Configuration Elements 252
- X.25 Access Background Information 253
  - Current X.25 Restrictions 255

Frame Relay Accesses 255
- Configuring a Frame Relay Access 255
  - Configuring General Access Information 255
  - Configuring a PVC 256
- Frame Relay General Configuration Elements 257
- Frame Relay PVC Configuration Elements 258
- Frame Relay Access Background Information 260
  - The Local Management Interface Overview 261
  - Data Rate Control Overview 261
  - Congestion Control Overview 262
  - Current Restrictions 262

Configuring Advanced Bridging 264

Overview 264
Bridge Dial Out 264
Configuring the Device List for Bridge Dial Out 265
Spanning Tree Protocol 266
Configuring Spanning Tree Protocol 266
Spanning Tree Protocol Configuration Elements 267
Spanning Tree Protocol Background Information 267
Bridge Mode of Operation 268
Configuring the Bridge Mode of Operation 268
Bridge Mode of Operation Configuration Elements 268
Bridge Mode of Operation Background Information 268
Unrestricted Bridge Mode 268
Restricted Bridge Mode 269
Bridge Filters 269
Configuring Bridge Filters 269
Bridge Filter Configuration Elements 272
Protocol Definition Configuration Elements 272
Bridge Filter Configuration Elements 272
Bridge Filters Background Information 273
Protocol Definitions 273
Bridge Filter Definitions 274
Dial Out Using Bridge Filters 283
Example: Bridge Dial Out Using a Destination MAC Address Filter 283
Known Connect List 285
Configuring the Known Connect List 285
Using CFGEDIT 285
Known Connect List Configuration Elements 286
Known Connect List Background Information 286

Configuring Advanced IP Routing 287

Overview 287
Static ARP Table Entries 288
Configuring Static ARP Table Entries 288
Static ARP Table Entries Configuration Elements 288
Static ARP Table Entries Background Information 288
The Isolated Mode 289
Configuring the Isolated Mode 289
Isolated Mode Configuration Elements 289
Isolated Mode Background Information 289
Static Route Lookup via RADIUS 289
Configuring Static Route Lookup via RADIUS 289
Static Route via RADIUS Configuration Elements 290
Static Route Lookup via RADIUS Background Information 290
IP Address Pool 290
Configuring an IP Address Pool 290
IP Address Pool Configuration Elements 290
IP Address Pool Background Information 291

IP Filters 291
Initiating the IP Filter Configuration 292
Configuring Packet Types 292
Configuring the Common IP Portion 293
Configuring TCP 294
Configuring UDP 294
Configuring ICMP 295
Configuring Forwarding Filters 296
Configuring Connection Filters 297
Configuring Exception Filter 298
Modifying the Final Condition for a Filter 299
Applying Filters 299
Applying Filters to Network Interfaces 299
Applying the Global Forwarding Filter 299
Applying per-device Forwarding Filters 299
IP Filters Configuration Elements 300
IP Filters Background Information 301
Filter Composition 302
Types of Filters 302
Role of Filters in the IP Processing Flow 303
Packet Types 304
Limitations 305
Example of an IP Filter Configuration 306
DHCP Relay Agent 308
Configuring a DHCP Relay Agent 308
DHCP Configuration Elements 309
DHCP Background Information 309
DHCP/BOOTP Relay Agent Environments 309
Example DHCP Configurations 311
DHCP Proxy Client 315
Configuring the DHCP Proxy Client 315
DHCP Configuration Elements 316
DHCP Background Information 316
Sample Configuration: IP Router with DHCP Proxy Client 317
Security Associations 318
Configuring Security Associations 318
DNS and NetBIOS Addresses 319
Configuring DNS and NetBIOS Addresses 319
DNS/NBNS Configuration Elements 320
DNS/NBNS Background Information 320

Configuring IPX 321
Overview 321
Configuring IPX Information 322
IPX Routing Option 323
Enabling/Disabling IPX 323
IPX Option Configuration Element 323
IPX Option Background Information 324
IPX Internal Network Number 324
Configuring the IPX Internal Network Number 324
IPX Internal Network Number Configuration Element 324
IPX Network Number Background Information 325

IPX Network Interfaces 325
Configuring IPX Network Interfaces 325
IPX Network Interface Configuration Elements 327
General IPX Network Interface Configuration Elements 327
RIP IPX Network Interface Configuration Elements 327
SAP IPX Network Interface Configuration Elements 328
IPX Network Interface Background Information 329
IPX Routing Protocols 330
Configuring IPX Routing Protocols 330
IPX Routing Protocol Configuration Elements 330
IPX Routing Protocol Background Information 331
Routing / Service Tables 331
Special Considerations - Remote LAN Interface 332
IPX Static Routes 333
Configuring IPX Static Routes 333
IPX Static Routes Configuration Elements 334
IPX Static Routes Background Information 334
IPX NetWare Static Services 335
Configuring IPX NetWare Static Services 335
IPX NetWare Static Services Configuration Elements 336
IPX NetWare Static Services Background Information 337
IPX Spoofing 337
Configuring IPX Spoofing 337
IPX Spoofing Configuration Elements 338
IPX Spoofing Background Information 338
Watchdog Protocol 339
SPX Protocol 339
IPX Type 20 Packet Handling 340
Configuring IPX Type 20 Packet Handling 340
IPX Type 20 Packet Handling Configuration Elements 340
IPX Type 20 Packet Handling Device Configuration Elements 341
IPX Type 20 Packet Handling Background Information 341
IPX Isolated Mode 341
Configuring IPX Isolated Mode 341
IPX Isolated Mode Configuration Elements 341
IPX Isolated Mode Background Information 341
IPX Triggered RIP / SAP 342
Displaying WAN Peer List 342
Configuring Triggered RIP / SAP Global Timers 342
Configuration Elements 343
Triggered RIP / SAP Background Information 343
IPX-Specific Information for Devices 344
Configuring IPX Devices 344
WAN Devices 344
Remote LAN Devices 346
IPX Configuration Elements for Devices 347
IPX Background Information for Devices 349
IPX Triggered RIP / SAP Device Background 349

Configuring SNMP 350

Overview 350
Configuring SNMP 350
SNMP Configuration Elements 352
SNMP Background Information 353
Using Cabletron NMS Systems 356

Configuring AppleTalk Routing 357

Overview 357
AppleTalk Routing Option 357
Enabling AppleTalk Routing 357
AppleTalk Routing Option Configuration Element 358
AppleTalk Routing Background Information 358
AppleTalk Ports 358
Configuring AppleTalk Ports 358
AppleTalk Ports Configuration Elements 359
AppleTalk Ports Background Information 360
The AppleTalk Network Type 360
Dynamic Node Address Assignment 360
The Zone Concept 361
AppleTalk Remote LAN 361
AppleTalk Static Routes 362
Configuring AppleTalk Static Routes 362
AppleTalk Routing Static Routes Configuration Elements 363
AppleTalk Routing Static Routes Background Information 363
AppleTalk Capacities 363
Configuring AppleTalk Capacities 363
AppleTalk Capacities Configuration Elements 363
AppleTalk Capacities Background Information 364
AppleTalk Isolated Mode 364
Configuring the AppleTalk Isolated Mode 364
AppleTalk Isolated Mode Configuration Elements 364

Configuring Call Control 365

Overview 365
Call Control Menu 365
Throughput Monitor 366
Configuring the Throughput Monitor 366
Throughput Monitor Configuration Elements 367
Throughput Monitor Background Information 367
Overload Condition Monitoring 368
Underload Condition Monitoring 369
Idle Condition Monitoring 369
Throughput Monitor Configuration Example 369
Call Interval Parameters 371
Configuring the Call Interval Parameters 371
Call Interval Configuration Elements 371
Call Interval Background Information 371
Monthly Call Charge 371
Configuring Monthly Call Charge 371
Monthly Call Charge Configuration Elements 372
Monthly Call Charge Background Information 372

Call Restrictions 372
Configuring Call Restrictions 372
Call Restriction Configuration Elements 373
Call Restrictions Background Information 376
Bandwidth Reservation 376
Configuring Bandwidth Reservation 376
Bandwidth Reservation Configuration Elements 378
Bandwidth Reservation Background Information 379
Semipermanent Connections 379
Configuring Semipermanent Connections 379
Semipermanent Connections Configuration Elements 381
Semipermanent Connections Background Information 381
Interactions with Other Features 381
CSM as a Call Control Manager 383
Configuring CSM for Call Control 383
Configuration Elements 383
Background Information 384
Call Control Management 384
Limitations / Considerations 385
D Channel Callback 385
Configuring D Channel Callback 385
D Channel Callback Configuration Elements 386
D Channel Callback Background Information 386
Digital Modem Inactivity Timeout 387
Configuring the Digital Modem Inactivity Timeout 387
Modem Inactivity Timeout Configuration Elements 387
Modem Inactivity Timeout Background Information 388

Configuring Other Advanced Options 389

Overview 389
The Digital Modem 389
Configuring for a Digital Modem 389
Digital Modem Background Information 390
Supported Modes of Connection 391
Relationships between Digital Modem and other Features 392
Default Async Protocol 392
PPP Mode 392
Terminal Mode 393
Call Disconnect 393
Default Async Protocol Configuration Elements 393
Background Information 394
Autosense Feature 395
Limitations 395
Interactions with Other Features 395
PPP Configuration 396
Configuring PPP 396
PPP Configuration Elements 396
PPP Background Information 398
PPP Link Failure Detection 398
PPP Reference Documents 399

Default Line Protocol 399
Configuring Default Line Protocol 399
Default Line Protocol Configuration Elements 400
Default Line Protocol Background Information 400
Log Options 400
Configuring Log Options 400
Log Options Configuration Elements 401
Log Options Background Information 402
Local Log File Overview 402
Syslog Server Overview 402
System Messages 404
Authentication Messages 404
Call Detail Recording 404
Compression Options 410
Configuring Compression Options 410
Compression Options Configuration Elements 411
Compression Options Background Information 412
Compression and CCP 412
TFTP 414
Configuring TFTP 414
TFTP Configuration Elements 414
TFTP Background Information 414
File Attributes 415
Configuring File Attributes 415
File Attributes Configuration Elements 415
File Attributes Background Information 416

VERIFICATION AND DIAGNOSIS 417

Verifying the Base System 418
Overview 418
Hardware Resources Operational? 418
WAN Adapter Initialized? 418
LAN Adapter Initialized? 419
WAN Lines Available for Use? 420
Verifying WAN Line Availability 420
Dedicated Serial Connections 421
LAN Connection Operational? 422
Bridge Initialized? 423
IP Router Initialized? 423
Remote Device Connectivity 424
Multi-Level Security 426
IP Host Mode 427
IP Host Initialized? 427
Verification 427
IP Host Mode Operational? 427
Verification over a LAN connection 428
Verification over a WAN connection 429

Alternate Accesses 429
Dedicated Connections 429
Frame Relay Connections 430
PPP Link Failure Detection 430
X.25 Connections 431
X.25 and a Terminal Server Menu 432

Verifying Routing Protocols 433

Overview 433
IP Routing Operational? 433
IP Routing Over a LAN Interface 433
IP Routing Over a WAN Interface 434
IP Routing Over a WAN (Direct Host) Interface 436
IP Routing Over a WAN Remote LAN Interface 438
IP Routing Over a WAN UnNumbered Interface 439
IP Filters 440
IP RIP Initialized? 441
IP RIP Output Processing on a LAN Interface 442
IP RIP Input Processing on a LAN Interface 443
IP RIP Output Processing on a WAN Interface 444
IP RIP Input Processing Operational on a WAN Interface 445
IPX 446
IPX Router Initialized? 446
IPX Routing Operational? 447
IPX Routing over a LAN Connection 447
IPX Remote LAN Connection 448
IPX Routing over a WAN Connection 450
Triggered RIP / SAP 450
AppleTalk Routing 452
AppleTalk Routing Initialized? 452
AppleTalk Routing Operational? 452
AppleTalk Routing over the LAN connection 453
AppleTalk Routing over a WAN connection 455

Verifying System Options 457

Overview 457
SNMP 457
Dial Out 459
Call Detail Recording 461
Compression 462
Reserved Bandwidth 463
DHCP Relay Agent 464
Verifying DHCP Relay Agent Initialization 464
Verifying the Relay Agent is Enabled 464
Verifying the Relay Agent is Operational 465
DHCP: Proxy Client 467
Verifying DHCP Proxy Client Initialization 467
Verifying the Proxy Client is Enabled 467
Verifying the Proxy Client is Operational 468
Verification of UDP Ports 468
Verification of IP Address Pool 469
D Channel Callback 469

Modem Callback 470
Verifying a Semipermanent Connection 471
Proxy ARP 472

TROUBLESHOOTING 474

LCD Messages 475
Overview 475
LCD Message Groups 475
Initialization LCD Message 475
Normal Operation LCD Messages 475
Error LCD Messages 476

System Messages 480
Overview 480
Informational Messages 481
Initialization Messages 481
Normal Operation Messages 481
Spanning Tree Messages 481
Warning Messages 481
Error Messages 481
System Message Summary 482

Trace Messages 544
Overview 544
Call Trace Messages 545
Call Trace Message Summary 546
IP Filters Trace Messages 551
PPP Packet Trace Messages 552
WAN FR_IETF Trace Messages 554
X.25 Trace Messages 554
X.25 Trace Message Summary 554
X.25 (LAPB) Trace Messages 557
X.25 (LAPB) Trace Message Summary 557

SYSTEM MAINTENANCE 559

Remote Management 560
Overview 560
SNMP 561
Installation and Configuration 562
Usage Instructions 562
Telnet 563
Installation and Configuration 564
Usage Instructions 564
WIN95 Dial-Up Networking 566
Setting up a New Number 566
Setting Up Server Type 566
Dialing Out 567

TFTP 568
Installation and Configuration 568
Usage Instructions 569
Carbon Copy 570
Installation and Configuration 570
Changing CARBON COPY Configuration Parameters 570
CARBON COPY Configuration Parameters for Modem Usage 571
Usage Instructions 572
Establishing a Remote Administration Session 572
Terminating a Remote Administration Session 573
Running without Carbon Copy 574
Removing Carbon Copy 575
Null Modem Connection 575
Adding Carbon Copy 575

System Commands 576
Overview 576
Accessing Administration Services 576
Setting the IP Address 577
Accessing Dynamic Management 577
Viewing Operational Information 578
Viewing Throughput Information 582
Throughput Monitor Contents 583
Saving Operational Information 584
Clearing Operational Information 584
Configuration-Related Commands 585
Terminating and Restarting the CyberSWITCH 585
Setting the Date and Time 586
Terminating Administration Sessions 586
AppleTalk Routing Commands 587
Bridge Commands 591
Call Control Commands 592
Call Detail Recording Commands 596
Call Restriction Commands 596
Compression Information Commands 597
CSM Commands 597
DHCP Commands 597
Digital Modem Commands 598
Frame Relay Commands 599
IP Routing Commands 601
IPX Routing Commands 605
ISDN Usage Commands 607
LAN Commands 608
Log Commands 608
Packet Capture Commands 609
RADIUS Commands 612
Serial Interface Commands 614
SNMP Commands 614
Spanning Tree Commands 614
Spanning Tree Port Information 614
Spanning Tree Bridge Information 615
TCP Commands 617

Telnet Commands 618
Terminal Commands 620
TFTP Commands 621
Trace Commands 622
UDP Commands 623
User Level Security Commands 623
WAN Commands 624
X.25 Commands 625

System Statistics 627
Overview 627
Connectivity Statistics 627
Call Restriction Statistics 628
Call Statistics 628
Throughput Monitoring Statistics 628
AppleTalk Statistics 629
AppleTalk Protocol Statistics 629
AppleTalk Data Delivery Protocol (DDP) Statistics 629
AppleTalk Echo Protocol (AEP) Statistics 630
AppleTalk Routing Table Maintenance Protocol (RTMP) Statistics 631
AppleTalk Zone Information Protocol (ZIP) Statistics 631
AppleTalk Name Binding Protocol (NBP) Statistics 632
AppleTalk Transaction Protocol (ATP) Statistics 632
AppleTalk Port Statistics 633
Bridge Statistics 634
Call Detail Recording Statistics 634
Compression Statistics 635
Compression Related Statistics 635
Decompression Related Statistics 635
DHCP Statistics 636
Common DHCP Statistics 636
DHCP Relay Agent Statistics 637
DHCP Proxy Client Statistics 638
Digital Modem Statistics 639
Frame Relay Statistics 639
Access Related Statistics 639
PVC Related Statistics 641
LAN Statistics 642
IP Statistics 643
IP Group Statistics 643
ICMP Group Statistics 645
IPX Statistics 646
IPX General Statistics 646
IPX Basic System Table Statistics 647
IPX Advanced System Table Statistics 648
IPX RIP Statistics 648
IPX Triggered RIP Statistics 649
IPX Route Statistics 649
IPX SAP Statistics 650
IPX Triggered SAP Statistics 650
IPX Service Statistics 651

RIP Statistics 651
RIP Global Statistics 651
RIP Interface Statistics 651
Serial Interface Statistics 652
SNMP Statistics 652
TCP Statistics 655
TFTP Statistics 656
Statistics for Server or Remote initiated TFTP Activity 656
Statistics for Local or Client Initiated TFTP Activity 656
Statistics for all TFTP Activity 657
UDP Statistics 658
WAN FR_IETF Statistics 658
WAN L1P Statistics 659
PRI S/T (T1/E1) Interface Statistics 659
Layer 1 PRI Error Statistics 659
Layer 1 General Statistics 660
WAN Statistics 660
X.25 Statistics 661
X.25 Access Related Statistics 661
X.25 Virtual Circuit (VC) Related Statistics 663

Routine Maintenance 665
Overview 665
Installing/Upgrading System Software 665
Executing Configuration Changes 665
Configuration Files 665
Making Changes Using CFGEDIT 665
Making Changes Using Manage Mode 666
Configuration Backup and Restore 666
Obtaining System Custom Information 666

APPENDICES 667

System Adapters 668
Ethernet Adapter 669
Basic Rate Adapter 670
Primary Rate Adapters 671
The PRI-8 671
The PRI-23 672
The PRI-23/30 673
Expander Adapter 674
V.35 Adapter 675
RS232 Adapter 676
Digital Modems 677
The DM-8 677
The DM-24 678
The DM-24+/DM-30+ 680
Encryption Adapter 682
DES Adapter (US Version) 682

System Worksheets 683
Network Topology 684
System Details 685
Resources 685
Lines 685
Accesses 686
Device Information 687
Bridging and Routing Information 688
Bridging 688
IP Routing 688
IPX Routing 689
AppleTalk Routing 690

CFGEDIT Map 691
Overview 691
Main Menu 691
Physical Resources Menu 692
Options Menu 693
Security Menu 696

Getting Assistance 699
Reporting Problems 699
Contacting Cabletron Systems 699

Administrative Console Commands Table 701

Manage Mode Commands Table 708

Cause Codes Table 712

INDEX 719

USING THIS GUIDE

The *User's Guide* is divided into the following parts:

SYSTEM OVERVIEW

We begin with an overview of bridging, routing, and specific CyberSWITCH features. Next, we provide an overview for both the system software and hardware.

SYSTEM INSTALLATION

In this segment of the *User's Guide* we provide guidelines for ordering ISDN service in the US, and a step-by-step description of installing hardware and upgrading software.

BASIC CONFIGURATION

We define basic configuration as the configuration needed by most devices. These are the areas of configuration that will get your system up and running. Note that not all configuration steps in this part are required. For example, if you are only using bridging, you will have no need to complete the configuration steps included in the chapter titled *Configuring Basic IP Routing*.

SECURITY CONFIGURATION

The CyberSWITCH provides a great variety of security options. For example, you may use device level security, user level security, or if preferred, no security. You may also perform authentication of a device / user in different ways. The security information may be stored on several different types of databases, either locally or on a variety of remote databases.

System security also allows the configuration of administrative session (Telnet session) enhancements. This provides secure access to the system along with flexible control.

ADVANCED CONFIGURATION

We define advanced configuration as a way to fine tune your system, or to configure options that are not necessarily needed by the majority of devices. For example, use this section to configure an alternate access, or to set up SNMP to manage your system.

VERIFICATION AND DIAGNOSIS

Once you've installed and configured your system, we recommend you verify its operational features. This segment describes how to verify (and then adjust, if necessary) the base system, protocols and options.

TROUBLESHOOTING

Troubleshooting includes a description of system LCD indicators, followed by system messages and trace messages. Each message listing in these chapters provides the message itself, a message definition, and where appropriate, possible corrective actions.

SYSTEM MAINTENANCE

In this section, we provide information to help you maintain your CyberSWITCH once it is operating. System maintenance information includes information regarding remote management, a chapter on both the system commands and the system statistics, and routine maintenance procedures.

APPENDICES

The *User's Guide* provides the following appendices:

NETWORK WORKSHEETS

These worksheets are provided to help you gather pertinent information for configuring your system. We recommend that you print copies of these blank forms and fill in the appropriate information before you begin configuring your system.

CFGEDIT MAP

This map provides a guide through the Configuration Editor structure, and may be a helpful reference when configuring the CyberSWITCH using the CFGEDIT utility.

GETTING ASSISTANCE

This appendix provides information for getting assistance if you run into problems when installing your system. A FAX form is included. You can print this form, fill out the information requested, and FAX it to Cabletron Systems, using the provided FAX number.

ADMINISTRATION CONSOLE COMMANDS

Provides a tabular listing of the system administration console commands and their uses.

MANAGE MODE COMMANDS

Provides a tabular listing of the Manage Mode commands and their uses.

CAUSE CODES

Provides a tabular listing of Q.931 Cause Codes and their meanings. These cause codes may appear in call trace messages.

SYSTEM ADAPTERS

Provides illustrations of available adapters for the CyberSWITCH.

DOCUMENTATION SET

This guide, the *User's Guide*, provides information to install and configure your system. It also provides information you may need to refer to keep your system running efficiently after it is up and running. For example, it provides a listing of system messages. Each message listing provides a definition of what the message means, and where appropriate, corrective action you can take. Many other subjects are covered, including routine maintenance, hardware information, system verification, and problem diagnosis.

This guide is one integral part of the entire documentation set. Please refer to the documents described below for additional information.

The *Example Networks Guide* includes several example networks, beginning with a simple network, and progressing to more complex networks. These example network chapters provide configuration instructions that you may find helpful in configuring your own similar network.

The *CSX7000 Guide* is a supplement to the *User's Guide*. Because the CSX7000 is a multi-system platform with many unique features, its hardware and monitoring capabilities vary widely from other Cabletron platforms. This guide details these differences.

The *Quick Start* provides abbreviated installation and configuration instructions for experienced users. Specific instructions for setting up various types of remote devices are also included.

The *RADIUS Authentication User's Guide* describes the setup of the RADIUS server software on a UNIX-based system. RADIUS (Remote Authentication Dial In User Service) provides multiple systems central database access for security authentication purposes. If you have Internet access, you may obtain this guide by following the steps outlined below:

- Use your Web browser to get to the following address:
  http:/ / service.nei.com
- From the resulting screen, click on *Anonymous.*
- Click on the *Radius* directory.
- Click on the *Docs* directory. The guide will be under this directory.

The *Release Notes* provide release highlights and important information related to this release. Access these notes via your Web browser:

`http://www.cabletron.com/support/relnotes`

When you initially install or upgrade your system, an abbreviated version of these notes are available for display. Or, after the system is operating, you may display them by issuing the *`list rel_note.txt`* console command.

GUIDE CONVENTIONS

The following conventions are used throughout the documentation:

System Commands
All system commands (Administration and Manage Mode commands) are italicized, and in a different font than the general text. For example, if you are instructed to enter the command to test for proper LAN connections, the command would appear as follows:

`lan stats`

CFGEDIT SCREENS
Screens that appear on the monitor as you are configuring your system using the CFGEDIT utility will be displayed using the style shown below:

```
Main Menu:

   1) Physical Resources
   2) Options
   3) Security
   4) Save Changes

Select function from above or <RET> to exit:
```

MONITOR DISPLAYS
Any messages or text that is displayed on your monitor will be shown in the style below:

```
LAN Port <port #> is now in the LISTENING state
WAN Port <port #> is now in the FORWARDING state
LAN Port <port #> is now in the LEARNING state
LAN Port <port #> is now in the FORWARDING state
```

DOCUMENTATION TITLES

All references to CyberSWITCH documentation titles will use the same font as normal text, but will be italicized. For example, all references to the User's Guide will appear as:

User's Guide

SYSTEM OVERVIEW

We include the following chapters in the *System Overview* segment of the *User's Guide.*

- *The CyberSWITCH*
  Provides the "big picture" view of a CyberSWITCH network. We include an overview of unique system features, interoperability, security, interfaces, system components, remote devices, and switches supported.

- *Hardware Overview*
  A description of system platforms and adapters.

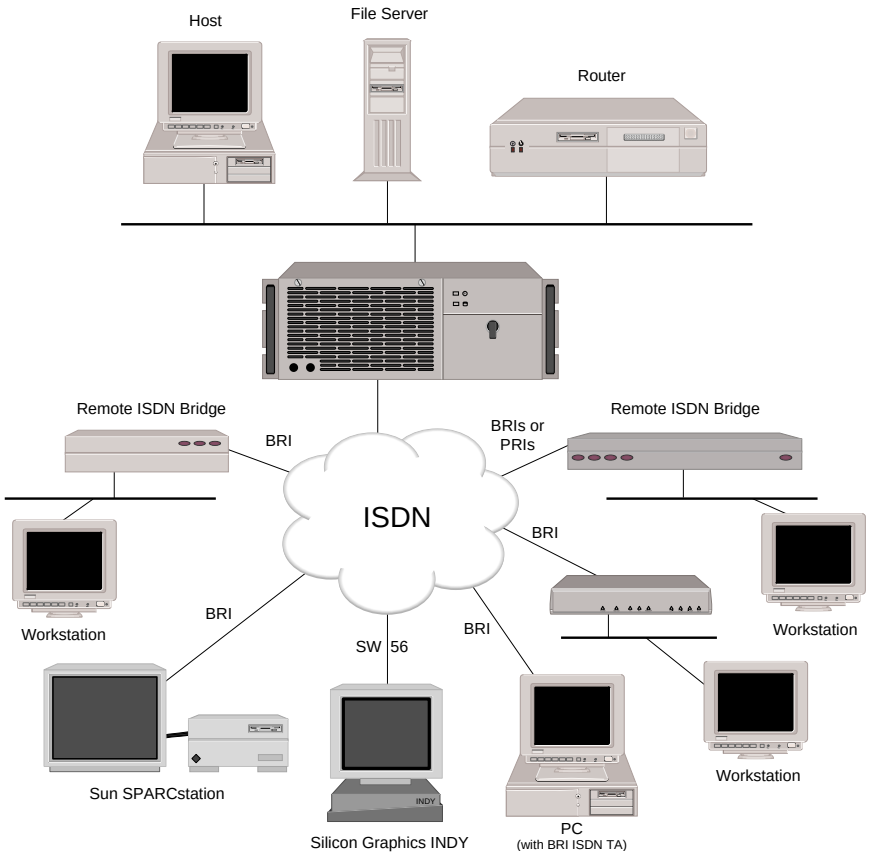
- *Software Overview*
  A description of the CyberSWITCH's system and administrative software. We also include a description of system files.

THE CYBERSWITCH

The CyberSWITCH family of products represents the latest in high-speed remote access hardware and software tools. These products allow customers to implement the connectivity solution ideally suited to the needs of their business - with support over a wide range of technologies covering both permanent and on-demand connections using ISDN, analog modem, Frame Relay, dedicated lines, and X.25.

The CyberSWITCH family of products can be used with a mix of bridges, routers, hosts, PCs, and workstations. These combinations provide internetworking capabilities that will allow devices to carry out LAN-to-LAN applications such as telecommuting, electronic mail, multi-media transmission, imaging, and CAD. Devices "dial up" into a single system using a multi-line hunt group to extend the capabilities offered by an enterprise LAN.

The CyberSWITCH's Central Site platforms utilize a built in CPU to manage analog and digital communications. The platforms consist of a number of modular slots that allow hardware customization. This hardware, along with the system's UAA software, work together to provide the centralized, concentrator function needed to support a variety of remote devices in a larger, Central Site environment.



UNIQUE SYSTEM FEATURES

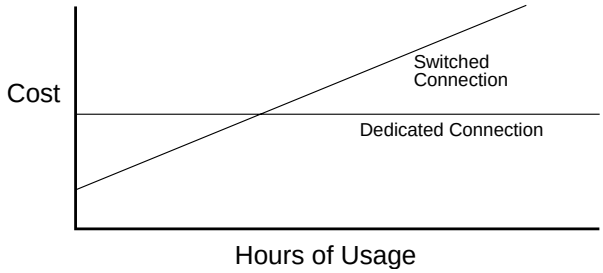
The CyberSWITCH combines unique features that improve cost-effectiveness, reliability, and performance for wide area network connections to remote devices. These features include:

- Bandwidth Agility
  The CyberSWITCH dynamically controls the bandwidth in use between itself and other PPP devices. This is accomplished by establishing and disconnecting calls. The number of calls is limited only by the types and number of lines available. The system monitors the connections for utilization and will add and remove the connections based on user-configurable throughput parameters. As network bandwidth requirements increase or decrease, the system will automatically adjust the number of network connections. Thus, your network costs will reflect the actual bandwidth being used.

- Filtering
  The CyberSWITCH's filtering feature allows you to control the flow of frames through the network. Filtering becomes necessary if you need to restrict remote access or control widespread transmission of sporadic messages. Customer-defined filters can forward messages based on addresses, protocol, or packet data.

- Combining Leased Line and Switched Connections
  Use the Switched Connections feature to automatically backup failed or overloaded leased lines (for example, in peak hour overflow situations). The capability of combining switched connections with leased line capacity allows you to reduce costs and greatly improve the reliability and performance of leased line networks.

  The following graph illustrates the relationship between cost and hours of usage when comparing a switched connection to a dedicated connection:



- Data Compression
  The CyberSWITCH can negotiate compression algorithms with another device on the network. After successfully negotiating compression, data is compressed by the remote device and transmitted to the CyberSWITCH system. The system decompresses the data, processes the information contained in the user data, and forwards the data as required. The system can receive data coming over a WAN or a LAN, and compress the data before transmitting it to another device on the network. The net effect is to increase interconnect bandwidth by decreasing transmission time. If negotiation for compression fails, data is transmitted uncompressed.

- Data Encryption
  The CyberSWITCH encryption option provides data encryption through the Data Encryption Standard (DES) algorithm. DES provides data security for transmissions over the WAN between encryption devices. Options are available for encrypting communications over point-to-point, frame relay, or Internet-based WANs. For more information, refer to the *Encryption Overview* and *IP Security* discussions.

  To activate the data encryption option on the CyberSWITCH, you will need to properly install and configure the encryption adapter on the system.

- Dial Out Capability
  The CyberSWITCH system will dial out to remote devices. This feature allows the system to accept user data received on the Ethernet LAN or ISDN network and initiate a data connection to the remote device specified in the user data. This allows devices on the local LAN to initiate connections to networks connected to the system over the switched digital network. The system monitors the connection for utilization and will remove the connection when it becomes idle.

- Digital Modem
  The CyberSWITCH's digital modem capability allows analog modems to be intermixed with ISDN, as required, to best fit specific networking needs. The digital modem adapter combines both hardware and software elements to support a number of modems on a single board (from eight V.34 modems to thirty K56Flex modems, depending upon adapter model). The digital modem feature conforms to the V.90 standard.

- Dynamic Management
  Manage Mode provides a "real-time" management mechanism that allows many system parameters to be changed without interrupting the current execution state of the system software. This feature consists of a series of console commands that enable a user to display current system parameters, change many parameters dynamically, and write changes to disk files so that they remain permanent.

- High Speed Digital Connections
  The CyberSWITCH system supports 56Kbps and 64Kbps connections to remote locations. These dial-up digital connections provide reliable high throughput connections for efficient data transfer for the same cost as analog connections. If any remote devices connected to the system support multi-link PPP, up to 32 parallel connections can be made at either 56Kbps or 64Kbps.

- IP Filters
  IP filters allow you to control the transmission of individual IP packets based on the packet type. You can specify packet type by IP address (source or destination) or by IP protocol (TCP, UDP, ICMP).

  Once you specify a packet type, two forms of IP filtering are available:
  - *Forwarding Filters*, applied at discrete points of the IP processing path to determine if a packet continues its normal processing, and a
  - *Connection Filter*, which determines if an IP packet requiring a WAN connection may continue.

- IP Security
  The CyberSWITCH encryption option implements Encapsulating Security Payload (ESP) protocol. ESP allows you to use CyberSWITCH nodes to implement a Secure Wide Area Network using the Internet as a backbone. ESP provides confidentiality of data transmissions using encryption to assure that packets intercepted during transit through the internet cannot be interpreted.

  The CyberSWITCH encryption option supports ESP Tunnel mode, in which an entire IP datagram (including its header) is encrypted and placed in a new IP datagram. This option provides the flexibility to choose which IP addresses must be sent encrypted data, and which may receive plain (unencrypted) data. The CyberSWITCH encryption option provides WAN connectivity for up to 92 B channels (with PRI and/or BRI connections).

- Link Layer Encryption
  The CyberSWITCH also provides the ability to do encryption at the PPP layer using Encryption Control Protocol with compatible devices.

- Multiple MAC/IP Addresses
  This feature allows two or more nodes to back up each other through the use of the Connection Services Manager (CSM).

  With this feature, two or more identically configured CyberSWITCH nodes on the same LAN can be monitored by CSM. Should CSM notice some condition which precludes one of the CyberSWITCH nodes from properly performing its function, it will order the other CyberSWITCH node to take over the other's duties by taking on its identity (i.e., its MAC and IP addresses).

- Packet Capture
  In order to monitor incoming LAN data, the CyberSWITCH packet capture feature will allow you to capture, display, save, and load bridged or routed data packets.

- Protocol Discrimination
  It is possible for multiple types of remote devices to use the same line. The system can determine the device type and the protocol encapsulation used by remote devices.

- RS232 Port: Dual Usage
  If your installation requires you to process PPP-Async data, this feature allows you to use the RS232 port for either console access or a serial data connection. This dual usage is possible through the CyberSWITCH's support of Autosense mode (the system default) and Terminal mode:
  - *Autosense mode* determines whether you are trying to connect using a VT emulation or PPP-Async, and connects you appropriately. (VT emulation requires you to perform four carriage returns to receive a login prompt.)
  - *Terminal mode* assumes that you only want to connect using VT emulation. A login prompt is displayed as soon as the connection is made.

- Security
  Security is a key issue for all central site network managers and is a priority with the CyberSWITCHs. The products provide high level features that help prevent unauthorized or inadvertent access to critical data and resources. They support extensive security levels including:
  - PPP PAP and CHAP

- User name and password
- Calling Line ID (CLID)
- Ethernet Address
- User Authentication
- Device Authentication
- Connection Services Manager (CSM)
- TACACS Client with Radius Server
- RADIUS
- Security Dynamic's ACE / SecurID

- Server Support
  The CyberSWITCH supports both Authentication and Accounting Servers. Authentication Servers provide a central database for networks with more than one CyberSWITCH. The central database consists of manageable, informational data (referred to as the Device List or Device Table). This data is accessed and used for authentication when a new connection is established to the system.

  The CyberSWITCH also supports a RADIUS Accounting Server to maintain accounting information, such as length of connections. This capability should be especially useful to Internet Service Providers.

- Simultaneous Connections
  The CyberSWITCH system supports simultaneous connections to multiple locations. These locations can connect by using different channels on the same line, or they can connect on different lines. This pooling of lines among many potential locations is more cost effective than alternative point-to-point lines.

INTEROPERABILITY OVERVIEW

"Interoperability" is the ability to operate and exchange information in a heterogeneous network. The CyberSWITCH supports interoperability with many different remote devices over ISDN.

INTEROPERABILITY PROTOCOLS

In order to communicate with various remote devices over ISDN, the CyberSWITCH must identify the device type and the protocol it is using.

The CyberSWITCH supports the following line protocols:
- HDLC Ethernet Frames
- Ordered Protocol for Ethernet Frames
- RFC1294 Based Encapsulation for IP Datagrams
- Point-to-Point Protocol (PPP) Encapsulation for IP Datagrams

The CyberSWITCH supports the following encryption protocols:
- Encapsulating Security Payload Protocol (ESP)
- Encryption Control Protocol (ECP)

The CyberSWITCH supports the following PPP protocols:
- Link Control Protocol (LCP)
- Multilink Protocol (MLP)

- Authentication Protocols
  - Challenge Handshake Authentication Protocol (CHAP)
  - Password Authentication Protocol (PAP)
- Network Control Protocols (NCP)
  - Internet Protocol Control Protocol for TCP / IP (IPCP)
  - Internetwork Packet Exchange Control Protocol for IPX (IPXCP)
  - Bridge Control Protocol for bridges (BCP)
- Compression Control Protocol (CCP)
- AppleTalk Control Protocol (ATCP)

The CyberSWITCH supports the following AppleTalk protocols:

- EtherTalk Link Access Protocol (ELAP)
- AppleTalk Address Resolution Protocol (AARP)
- PPP AppleTalk / AppleTalk Control Protocol (ATCP)
- Datagram Delivery Protocol (DDP)
- Routing Table Maintenance Protocol (RTMP)
- AppleTalk Echo Protocol (AEP)
- Name Binding Protocol (NBP)
- Zone Information Protocol (ZIP)

INTEROPERABILITY DEVICES

Remote devices that may connect to the CyberSWITCH include the following:

- MAC Layer Bridges
- IP Host Devices
- IP Router Devices
- IPX Routers
- AppleTalk Routers

MAC layer bridges connect to the system using the HDLC bridge encapsulation line protocol. These devices send transparently bridged Ethernet frames to the system. MAC layer bridges do not process network layer protocols. They forward all packets based on source and destination MAC addresses.

IP Host devices are single workstations or PCs that connect to the system at the IP network layer. These devices use either the RFC1294 based protocol or PPP to communicate with the system.

IP router devices are single devices that represent many other IP hosts and routers to the system. They must use the CHAP or PAP protocol to identify themselves to the system. IP routers usually provide IP network address information at connection time (and use PPP to send user data to the system).

IPX routers are single devices that perform network layer tasks (addressing, routing, and switching) to move packets from one location on the network to another. IPX routers use the Internetwork Packet Exchange (IPX) protocol, typical of the NetWare environment.

AppleTalk routers route AppleTalk datagrams based on address information. They support the following protocols: RTMP, NBP, and ZIP.

ENCRYPTION OVERVIEW

Cabletron's encryption options provide two popular approaches for encrypting WAN communications, each with distinct advantages in certain applications. These options are: Network Layer Encryption and Link Layer Encryption.

NETWORK LAYER

Cabletron's Network Layer Encryption is an IP Security-based form of encryption. IP Security (IPSec) can potentially reside in many devices within the network. Since IPSec is specific to IP, data must be contained in an IP datagram in order for encryption to take place. This also implies that an IPSec-compliant switch or router must perform network-layer routing. A device which does not perform network-layer processing (such as a pure bridge) will not be capable of IPSec-based encryption. Non-IP protocols such as IPX and AppleTalk must be encapsulated within IP in order to take advantage of IPSec.

IPSec is primarily aimed at providing secure communications across IP networks such as the Internet. Data can traverse multiple intermediate (untrusted) nodes (such as Internet backbone routers) while still ensuring strong data security. But it can also be applied in point-to-point networks where the layer-3 protocol is IP (for example, IP transported across the WAN using PPP).

Network-layer encryption works as follows:
IP datagrams transmitted from one LAN to another LAN funnel through a CyberSWITCH node where they are encrypted and encapsulated. The destination address on the encapsulated datagram is that of the CyberSWITCH node servicing the other trusted subnet.

When the IP datagram reaches the destination CyberSWITCH node, the Encapsulating Security Payload (ESP) header is removed, the ESP payload is decrypted, and the original IP datagram is forwarded to its original destination.

CyberSWITCH encryption requires additional *Security Association* information that can be supplied through CFGEDIT. Each security association identifies a range of IP addresses, encryption parameters to be used to encrypt communications to those IP addresses, and the IP address of the peer CyberSWITCH (or other ESP node) responsible for decrypting the communications. The peer will have knowledge of the same security association.

Security associations between peer CyberSWITCH nodes are identified by a Security Parameter Index (SPI), which is a 32-bit number. The SPI is transmitted in the ESP header and is used by the peer CyberSWITCH node to identify the necessary information to decrypt the ESP payload.

IP datagrams to these IP destination addresses are encrypted and encapsulated with an ESP header. The ESP header indicates a destination address of an intermediate CyberSWITCH node which will be responsible for decrypting and decapsulating these packets before sending them on to their intended destination.

LINK LAYER

Link layer encryption occurs at layer 2 of the ISO networking model. In the case of a WAN, PPP acts as a layer 2 protocol. Encryption Control Protocol (ECP) serves to handle encryption of a PPP datagram.

Link layer encryption is independent of any network layer protocols. Since PPP provides transport of IP, IPX, AppleTalk, and other protocols, link layer encryption based on ECP provides multi-protocol encryption by default. Devices implementing it can act as routers or bridges, as long as the underlying WAN protocol is PPP.

To use link layer encryption, the connection between encrypting and decrypting devices must truly be point-to-point. This includes ISDN dial-up connections, or point-to-point dedicated lines.

SECURITY OVERVIEW

The system provides several options for validating remote devices and for managing network security. The security options available are dependent on the remote device type, type of access, and the level of security required.

Levels of security include no security, device level security, user level security, and multi-level security. Device level security is an authentication process between devices, based on protocol and preconfigured information. Security information is configured either in the system's On-node Device Database, or in a central database such CSM. Here the network administrator specifies all of the security information for each individual user. A portion of this information is used to identify the remote device. The remaining data is used to perform user validation after user identification has been completed.

User level security is an interactive process. It is currently supported on the system through the TACACS or ACE server programmed for use with security token cards. With user level security, the potential network user explicitly connects to the server and must properly "converse" with it in order to connect with other devices beyond the server.

Important to user level authentication is the security token card. This card, programmed in conjunction with the authentication server, generates random passwords. These passwords must be supplied correctly at system login time, or access to the network will be denied. The security token cards should be issued to each user on the network to properly maintain system integrity.

Multi-level security provides device level security for all remote devices. Individual devices may be configured for user level authentication as well. In this case, device level authentication takes place between the system and the remote device. Then a specific user must initiate user level authentication by starting a Telnet session. Both levels of authentication must be satisfied before traffic can pass.

NETWORK INTERFACE OVERVIEW

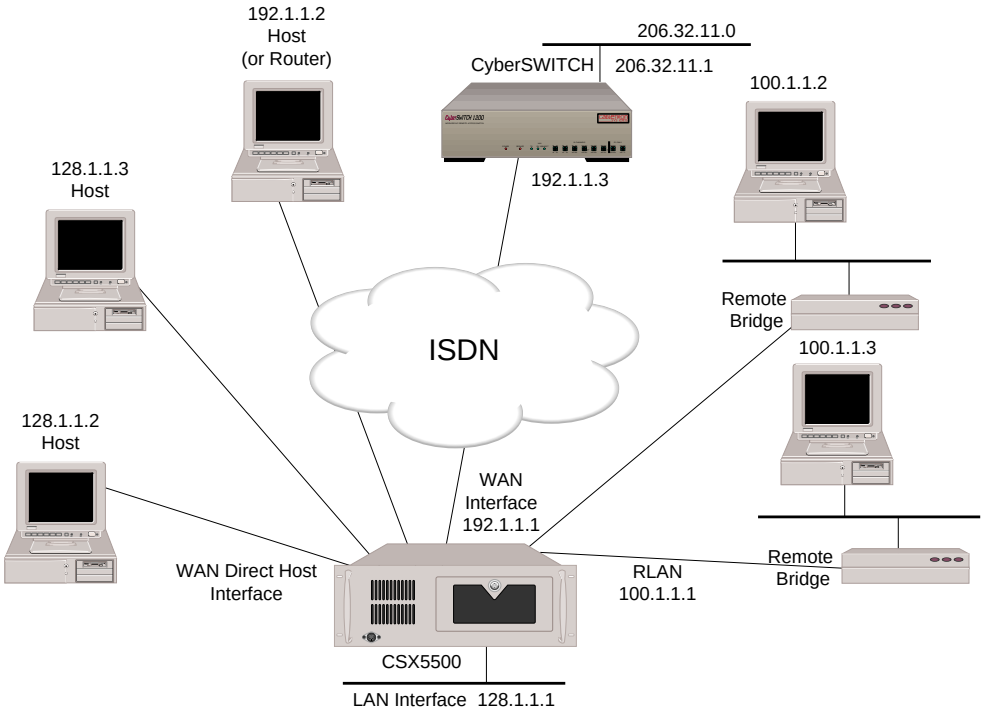
The network interface is the physical connection of the CyberSWITCH to a data network. For example, the Ethernet resource in the system provides a network interface to an Ethernet LAN. The ISDN lines in the system provide network interfaces to multiple remote networks. Because of their switched nature, the ISDN lines provide virtual network interfaces. That is, the same physical ISDN line can actually connect to different remote networks by dialing a different phone number.

The CyberSWITCH provides a set of network interfaces that give you a wide range of flexibility. The network interfaces provided by the system are:

- LAN IP Network Interface
- LAN IPX Network Interface

- WAN IP Network Interface
- WAN (Direct Host) IP Network Interface
- WAN RLAN IP Network Interface
- WAN RLAN IPX Network Interface
- WAN (UnNumbered) Network Interface

The variety of network interfaces allows the installation of a wide range of devices at remote sites. As illustrated below, you can simultaneously choose bridges, routers, or host devices based on the specific remote site requirements.



In the diagram above, the LAN Interface 128.1.1.1 is attached to the IP network 128.1.0.0. The WAN Direct Host Interface represents LAN Interface 128.1.1.1 and allows the remote IP hosts to share the network address space of 128.1.0.0. The WAN Interface 192.1.1.1 is logically attached to the IP network 192.1.1.0. The RLAN Interface 100.1.1.1 is logically attached to the IP network 100.1.1.0.

SYSTEM COMPONENTS

The major components of the CyberSWITCH are:

- System hardware consisting of a platform, an administration port provided by the platform, and adapters.
- System software specific to the CyberSWITCH, adapter modules, and administration functions.
- Administration software that provides configuration, diagnostics and maintenance on the system.
- System files containing configuration and operational information.
- Remote ISDN devices which interoperate with the system and allow device access to network resources.

More detailed descriptions of system software and hardware are included in the next two chapters. The following section describes remote ISDN devices.

REMOTE ISDN DEVICES

The CyberSWITCH provides a centralized concentrator function for remote ISDN devices. The devices can be separated into the following categories:

- remote ISDN bridge devices
- PC based terminal adapters
- ISDN enabled workstations
- other ISDN routers

Typical remote ISDN bridges provide one Ethernet port and one basic rate ISDN port. The basic rate port is connected to the switched digital network and is used to make connections to the CyberSWITCH. The Ethernet port is used to connect to a remote LAN. The remote bridge device sends Ethernet frames from devices on the remote LAN over the switched network.

PC-based terminal adapters connect to a remote personal computer and use the switched digital network to connect to the system. The terminal adapter sends network protocol specific frames from the host PC device over the switched network.

Workstation-based terminal adapters connect to a workstation and use the switched digital network to connect to the system. The terminal adapter sends network protocol specific frames from the workstation over the switched network.

SWITCHES SUPPORTED

Switch types supported by the CyberSWITCH's basic rate and primary rate ISDN adapters:

Type of Switch	*Basic Rate*	*Primary Rate*
AT&T #4ESS	NA	Yes
AT&T #5ESS	Yes	Yes
AT&T Definity	Yes	Yes
AT&T Legend	Yes	NA
NET3	Yes	NA
NET5	NA	Yes
NT DMS 100	Yes	Yes
NT DMS 250	NA	Yes
NT DMS 500	NA	Yes
NT SL-100	Yes	Yes
NTT	Yes	Yes
NI-1	Yes	NA
TS013	Yes	NA
TS014	NA	Yes
1TR6	Yes	Yes

Switch support may vary from country to country. Use the following as a guideline:

Country	*Switches supported (BRI lines)*	*Switches supported (PRI lines)*
Australia	TS013 NET3	TS014 NET5
Germany	1TR6 NET3	1TR6 NET5
Japan	NTT	NTT
United States	AT&T 5ESS AT&T Definity AT&T Legend NT DMS 100 NI-1	AT&T 4ESS AT&T 5ESS AT&T Definity NT DMS 100 NT DMS 250 NT DMS 500 NT SL-100
International	NET3	NET5

HARDWARE OVERVIEW

The product you have purchased is integrated on the following platforms: the CSX5500, CSX6000, and CSX7000. Through the use of adapters, these platforms support remote routing and bridging of local area networks using ISDN BRI or PRI services. Options also include V.35, RS232, encryption adapters, and Digital Modem connections.

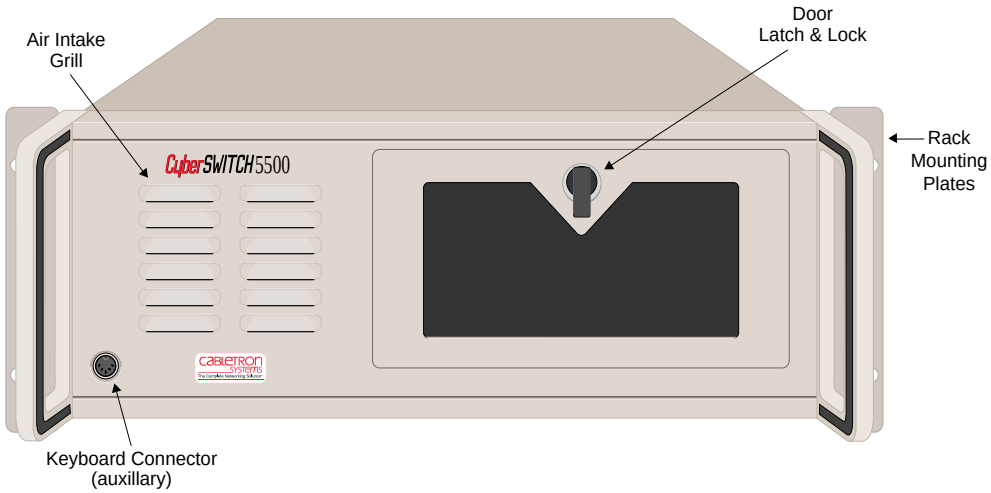
This chapter provides a description of system platforms and adapters. We also include descriptions of several products that we support that were produced by Network Express.

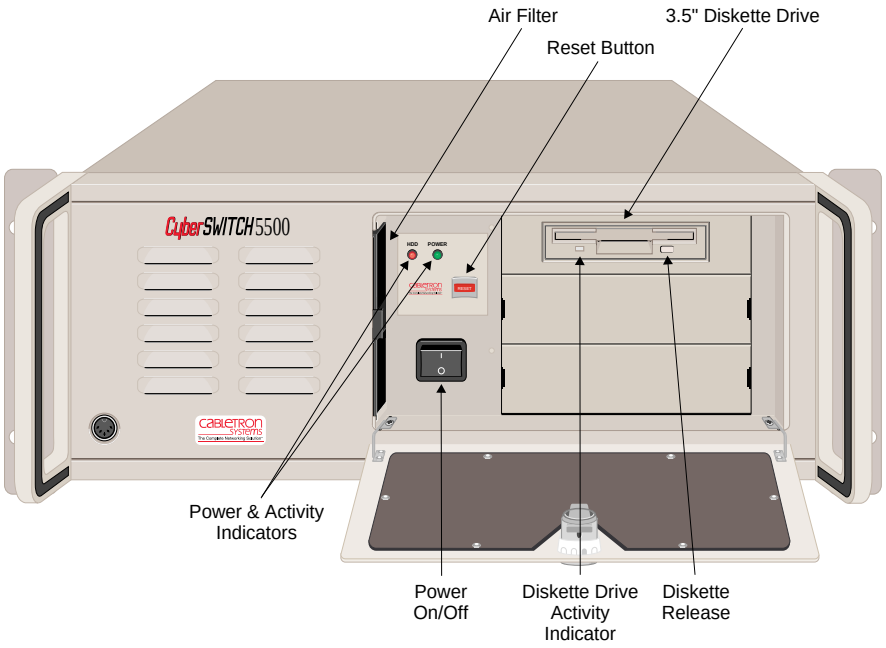
SYSTEM PLATFORMS

The CyberSWITCH consists of a main processor and system memory. The type of processor and the number of available slots vary by model. (See table.) The front of the platform has a diskette drive, control buttons, LED indicators and an LCD display. Connectors for the power, the LAN, and the network are all located on the back of the chassis. Administration ports for local and remote administration console attachments are also located on the back of the chassis.

Platform	*Number of Slots*	*Main Processor*	*Speed*
CSX5500	6	Pentium	133 MHz
CSX6000	8	Pentium	90 MHz
CSX7000	16	Pentium	133 MHz
NE 2000-II	3	i486	25 MHz
NE 4000	6	i486	33 MHz
NE 5000	8	i486	66 MHz

THE CSX5500



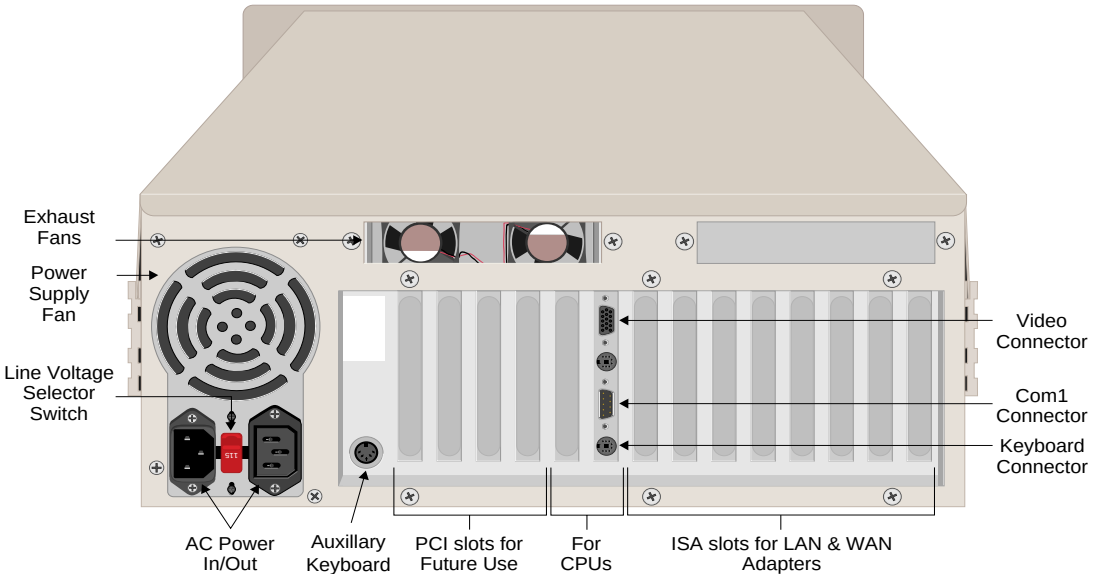


PLATFORM DESCRIPTION

The CSX5500 is a high capacity, central site communications platform. This platform is a LAN / WAN bridge / router built to accommodate multiple WAN technologies. It supports up to 16 ISDN BRI ports or 4 PRI ports, 2 digital modem cards, V.35, Frame Relay and Dedicated Lines services. It supports TCP / IP, IPX, and AppleTalk, as well as ML-PPP and compression. It has single or dual port Ethernet capability. The CSX5500 utilizes a CPU with 133 MHz Pentium processing.

The CSX5500 is a rack-mountable platform. The front panel has an air-intake grill, an auxiliary keyboard jack, and a peripheral access door, which may be latched. The activity indicators for power-on and disk activity, diskette drive, and control buttons are located behind the access door.

The back of the chassis has mountings for a RS-232 serial port, and connectors for a keyboard and monitor. The chassis has eight ISA slots for LAN and WAN adapters. However, because of power and cooling restrictions, we limit the number of usable adapter slots to five (one for a LAN adapter, and up to four for WAN adapters).



CLEANING THE CSX5500 AIR FILTER

The CSX5500 has a removable air filter. This filter is provided to ensure system cleanliness and stability in dusty operating environments. The filter is located just behind the left side of the chassis' front panel. For best performance (and as an alternative to replacement) regularly wash the filter in warm water and a mild detergent.

Before removing the air filter for cleaning, read the following warning and caution notes.

WARNING

Before removing the air filter for cleaning, ensure that the system is powered off and the power cord is unplugged from the power source. Note that the Power ON / OFF switch does not disconnect the power from the system. Failure to unplug the power cord can result in serious injury or equipment damage.

CAUTION

An electrostatic discharge (ESD) can damage your system. We recommend that you perform this procedure only at an ESD workstation. If such a workstation is unavailable, provide some ESD protection by wearing an antistatic wrist strap attached to chassis ground when handling components.

To clean the air filter:

1. Power down the system and disconnect the system's power cord from the power source.
2. Open the door located on the right side of the front chassis.
3. Once the door is opened, you can slide the air filter out from the left side of the chassis.
4. Once removed, clean the filter by washing it in warm water and a mild detergent. Make sure it is completely dry before you place it back in the system.
5. Slide the filter back into place.
6. Close the chassis door.
7. Reconnect the power cord and power up the system.

PLATFORM CHARACTERISTICS

Physical Characteristics

Height:	171.5 mm (6.86 in)
Width:	430 mm (17.2 in)
Depth:	483 mm (19.32 in)
Weight:	18 kg maximum (40 lb. maximum)

Environmental Characteristics

Operating Temp:	0° to 55° C (32° to 131° F)
Operating Humidity:	5 to 95% non-condensing
Operating Altitude:	3048 m maximum (10,000 ft maximum)
Non-operating Shock:	40 G, 11 ms 1/2 sine wave
Storage Temperature:	0° to 70° C (32° to 158° F)

Electrical AC Power Input

Voltage:	90 - 120 V	Current:5 A
Voltage:	180 - 265 V	Current:4 A
Frequency:	47 - 63 Hz	

Regulatory Compliance

Meets or exceeds the following:

Safety:	UL 1950, CSA C22.2 No. 950, EN 60950, IEC 950, and 72/23/EEC
EMI:	FCC Part 15, EN 55022, CSA 108.8, EN 50082-1, VCCI V-3, and 89/336/EEC

Rack Mounting:

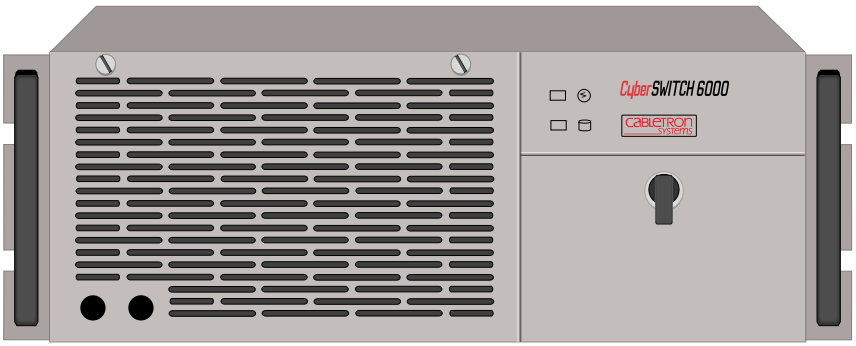
475 mm (19 inch) Industrial Rack Mount Chassis meets EIA RS-310C standard

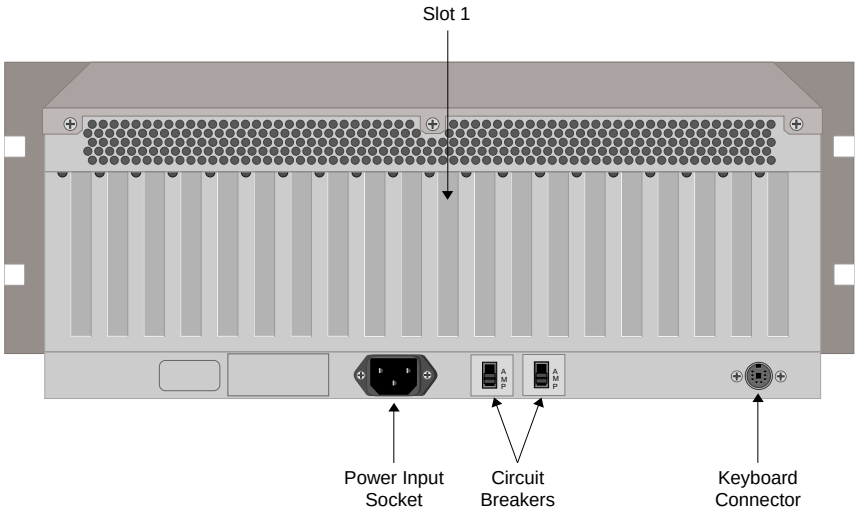
CAUTION FOR DC-POWERED CSX5500S

To reduce the risk of electrical shock or energy hazards:

- Connect to a reliably-grounded SELV source.
- Use branch circuit overcurrent protection rated at 15A only.
- Use 12 or 14 AWG conductors only.
- Incorporate a readily-accessible disconnect device in the field wiring that is suitably approved and rated.
- Install in a restricted access area in accordance with the NEC or the authority having jurisdiction.

THE CSX6000





PLATFORM DESCRIPTION

The CSX6000 is a high density, modular, central-site communications platform. It utilizes a built in CPU with 90 MHz Pentium processing.

The CSX6000 is a rack-mountable platform. The front panel has the activity indicators for power-on and disk activity, an air-intake grill, and a peripheral access door, which may be latched or locked closed. The diskette drive, control buttons, and an LCD display are located behind the access door. On the back of the chassis, the rear panel has mountings for a RS-232 serial port, and connectors for a keyboard and monitor.

The CPU is located in the center of the chassis in the one ISA + PCI slot (labelled *slot 1* in the back panel illustration). There are nine additional ISA slots for adapters to the right of the CPU board. However, because of power and cooling restrictions, we limit the number of usable adapter slots to seven (one for a LAN adapter, and up to six for WAN adapters).

CLEANING THE CSX6000 AIR FILTER

The CSX6000 has a removable air filter. This filter is provided to ensure system cleanliness and stability in dusty operating environments. The filter is located just behind the chassis' front panel. For best performance (and as an alternative to replacement) regularly wash the filter in warm water and a mild detergent.

Before removing the air filter for cleaning, read the following warning and caution notes.

WARNING

Before removing the air filter for cleaning, ensure that the system is powered off and the power cord is unplugged from the power source. Note that the Power ON / OFF switch does not disconnect the power from the system. Failure to unplug the power cord can result in serious injury or equipment damage.

CAUTION

An electrostatic discharge (ESD) can damage your system. We recommend that you perform this procedure only at an ESD workstation. If such a workstation is unavailable, provide some ESD protection by wearing an antistatic wrist strap attached to chassis ground when handling components.

To clean the air filter:

1. Power down the system and disconnect the system's power cord from the power source.
2. Turn the four quarter-turn screws securing the front panel to the chassis.
3. Remove the front panel to access the fan filter.
4. Remove the fan filter.
5. Once removed, clean the filter by washing it in warm water and a mild detergent. Make sure it is completely dry before you place it back in the system.
6. Reposition the filter and the front panel.
7. Tighten the four front panel quarter-turn screws.
8. Reconnect the power cord and power up the system.

PLATFORM CHARACTERISTICS

Physical Characteristics

Height:	178 mm (7.0 in)
Width:	482.6 mm (19.0 in)
Depth:	558.8 mm (22 in)
Weight:	18 kg maximum (40 lb. maximum)

Environmental Characteristics

Operating Temp:	0° to 55° C (32° to 131° F)
Operating Humidity:	5 to 95% non-condensing
Operating Altitude:	3048 m maximum (10,000 ft maximum)
Non-operating Shock:	40 G, 11 ms 1/2 sine wave
Storage Temperature:	0° to 70° C (32° to 158° F)

Electrical AC Power Input

Voltage:	90 - 120 V	Current:5 A
Voltage:	180 - 265 V	Current:4 A
Frequency:	47 - 63 Hz	

Regulatory Compliance

Meets or exceeds the following:

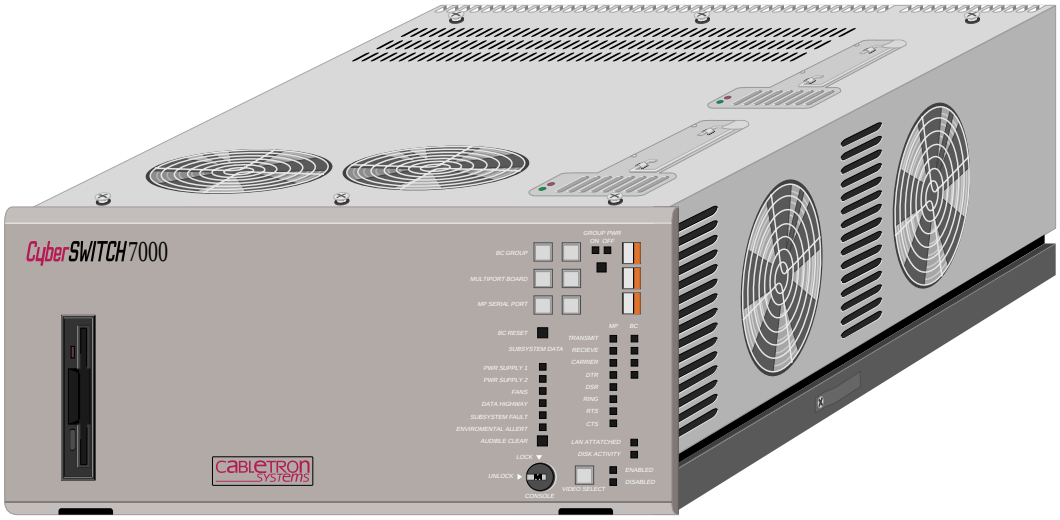
Safety:	UL 1950, CSA C22.2 No. 950, EN 60950, IEC 950, and 72/23/EEC
EMI:	FCC Part 15, EN 55022, CSA 108.8, EN 50082-1, VCCI V-3, and 89/336/EEC

CAUTION FOR DC-POWERED CSX6000S

To reduce the risk of electrical shock or energy hazards:

- Connect to a reliably-grounded SELV source.
- Use branch circuit overcurrent protection rated at 15A only.
- Use 12 or 14 AWG conductors only.
- Incorporate a readily-accessible disconnect device in the field wiring that is suitably approved and rated.
- Install in a restricted access area in accordance with the NEC or the authority having jurisdiction.

THE CSX7000



PLATFORM DESCRIPTION

The CSX7000 is designed for large, central sites and Internet Service Providers. It is a high availability, remote access switch that offers modularity and flexibility for these large sites.

The CSX7000 consists of a *platform*, *processor modules*, and an *Environmental Management System Module*, and includes environmental management of one or more platforms. It is capable of containing multiple processor modules (for backup or additional line capacity) in the platform's 16-slot backplane. The CSX7000 may also support other servers, including authentication servers.

Currently, a single CSX7000 platform supports a maximum of four processor modules (or *system groups*) at a time. Each system group supports a maximum of one Processor Module card, one LAN, and six WAN cards. (Of course, four fully-maximized system groups would not fit into the 16-slot backplane). Up to 31 CSX7000 platforms may be daisy-chained together to form a cluster.

Because of its unique platform features, the CSX7000 is described in further detail in the *CSX7000 Guide*.

PLATFORM CHARACTERISTICS

Environmental Characteristics

Operating Temperature:	0° to 45° C (32° to 113° F)
Storage Temperature:	-20°+70°C
Operating Humidity:	20-85% non-condensing
Operating Altitude:	Up to 3048 m max (10,000 ft max.)
Non-operating Shock:	40 G, 11 ms

Physical Characteristics

Height:	218 mm (8.60 in)
Width:	483 mm (19.0 in)
Depth:	641 mm (25.25 in)
Weight:	36 kg max. (80 lb. max.)

Power Supply Specifications

350 Watt power supply; two versions with different input AC voltages:

- *Version 1*

AC Input Voltage:	90 to 135 V
AC Input Current:	7.5 A
AC Input Frequency:	47 - 63 Hz

- *Version 2*

AC Input Voltage:	180 to 264 V
AC Input Current:	4.0 A
AC Input Frequency:	47 to 63 Hz

Regulatory Compliance

Meets or exceeds the following:

Safety:	UL 1950, CSA C22.2 No. 950, EN 60950, IEC 950, and 72/23/EEC
EMI:	FCC Part 15, EN 55022, CSA 108.8, EN 50082-1, VCCI V-3, and 89/336/EEC

Disk Drives

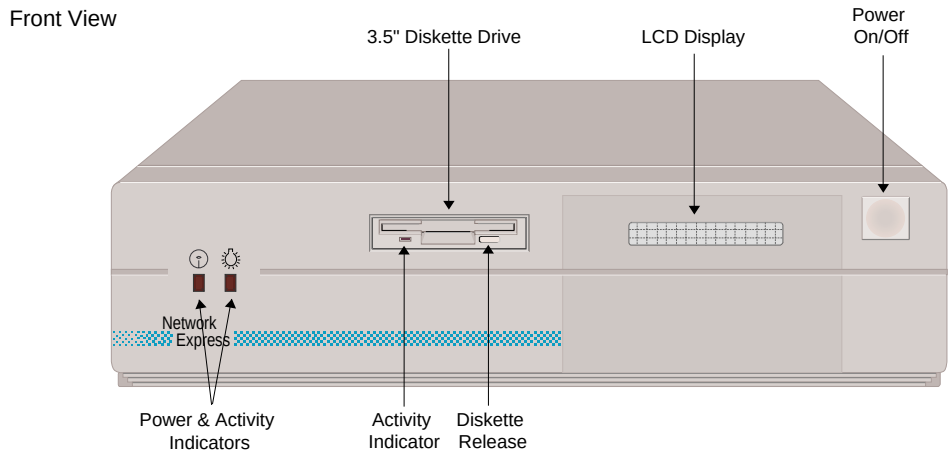
Number of 1/3 height, IDE disk drives supported:	8

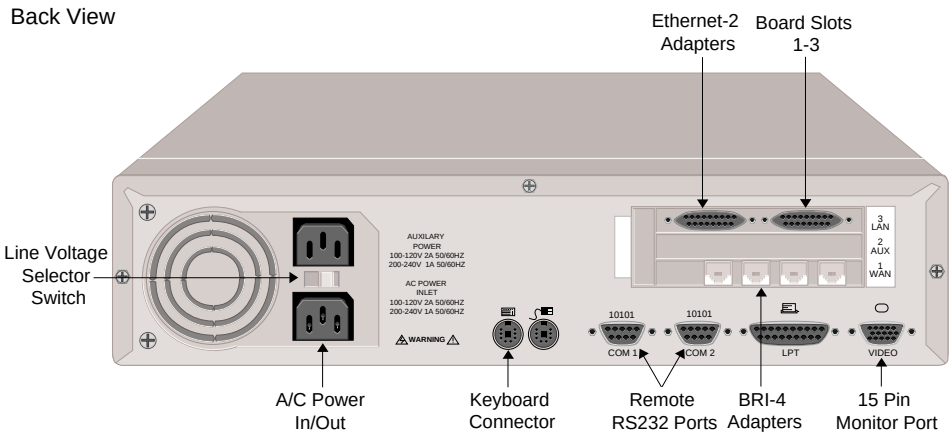
CAUTION FOR DC-POWERED CSX7000S

To reduce the risk of electrical shock or energy hazards:

- Connect to a reliably-grounded SELV source.
- Use branch circuit overcurrent protection rated at 15A only.
- Use 12 or 14 AWG conductors only.
- Incorporate a readily-accessible disconnect device in the field wiring that is suitably approved and rated.
- Install in a restricted access area in accordance with the NEC or the authority having jurisdiction.

THE NE 2000-II (A NETWORK EXPRESS PLATFORM)





PLATFORM DESCRIPTION

The NE 2000-II platform has three slots for adapters. This platform is small enough in size to be suitable for an office environment or to fit into a communications rack. The front has a diskette drive, control buttons and an LCD display. The display presents continuous status and error information.

Connectors for the power, the LAN, and the network are all located on the back of the chassis. An administrative port (shown as the Remote RS232 Port on the figure), and ports for an optional local monitor and keyboard are also located on the back of the chassis.

PLATFORM CHARACTERISTICS

Physical Characteristics

Height:	107 mm (4.2 in)
Width:	437 mm (17.2 in)
Depth:	411 mm (16.2 in)
Weight:	9 kg (20 lb)

Environmental Characteristics

Operating Temp:	10° to 35° C (50° to 95° F)
Operating Humidity:	20 - 80% non-condensing
Operating Altitude:	3,048 m maximum (10,000 ft maximum)
Non-operating Shock:	30 G, 11 ms, 1/2 sinewave
Storage Temperature:	40°^{o} to 70°^{o} C (-40° to 158° F)

Electrical AC Power Input

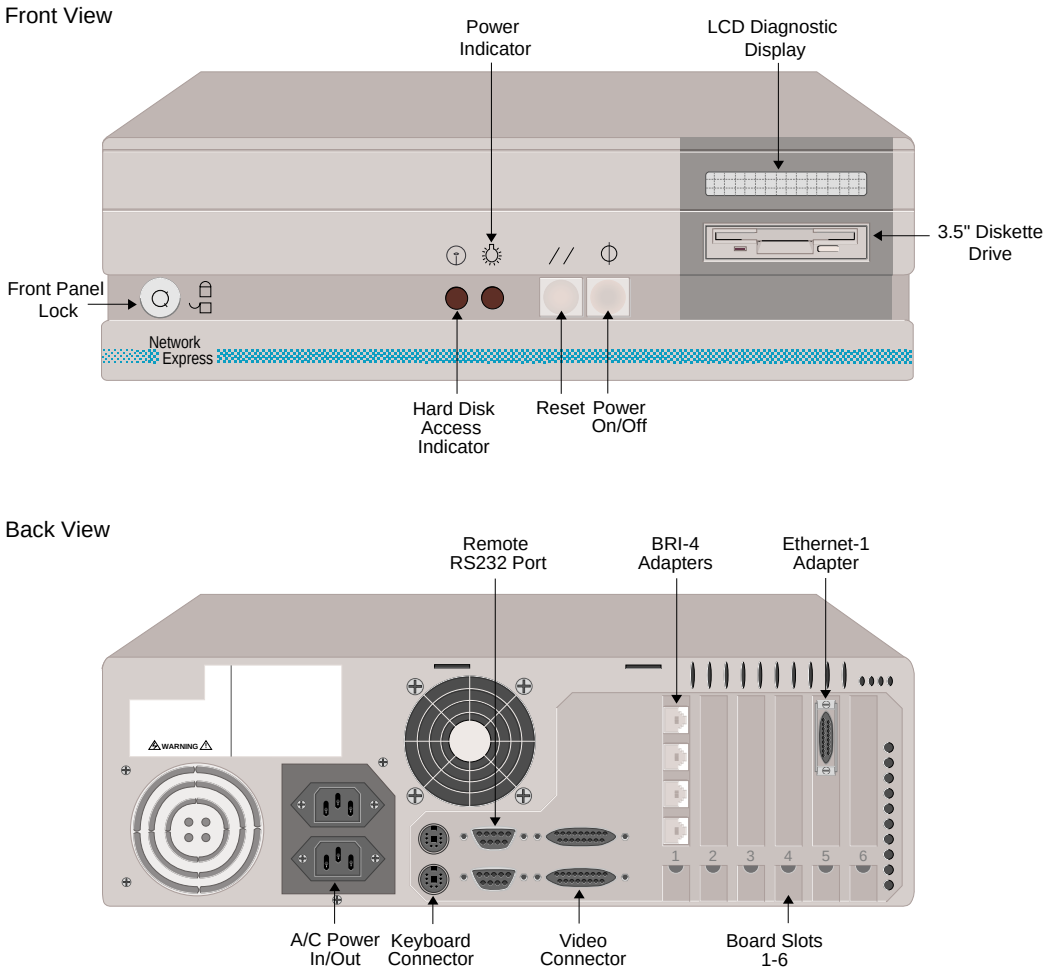
Voltage:	90 - 132 V	Current:5 A
Voltage:	180 - 264 V	Current:3 A
Frequency:	47 - 63 Hz	

Regulatory Compliance

Meets or exceeds the following:

Safety:	UL 1950, CSA C22.2 No. 950, EN 60950, IEC 950, and 72/23/EEC
EMI:	FCC Part 15, EN 55022, CSA 108.8, EN 50082-1, VCCI V-3, and 89/336/EEC

THE NE 4000 (A NETWORK EXPRESS PLATFORM)



PLATFORM DESCRIPTION

The NE 4000 platform has six slots for adapters. You can place the platform either on its feet or standing on a side. The front has a diskette drive, control buttons and an LCD display. The display presents continuous status and error information. Connectors for the power, the LAN, T1 interface, BRI, mouse, keyboard and monitor are all located on the back of the chassis.

PLATFORM CHARACTERISTICS

Physical Characteristics

Height:	158 mm (6.22 in)
Width:	439 mm (17.3 in)
Depth:	434 mm (17.08 in)
Weight:	17.23 kg (38 lb)

Environmental Characteristics

Operating Temp:	10° to 35° C (50° to 95° F)
Operating Humidity:	80% non-condensing
Operating Altitude:	3,048 m maximum (10,000 ft maximum)
Non-operating Shock:	30 G, 11 ms, 1/2 sinewave
Storage Temperature:	-40° to 65° C (-40° to 149° F)

Electrical AC Power Input

Voltage:	100 - 120 V	Current: 8 A
Voltage:	200 - 240 V	Current: 5 A
Frequency:	47 - 63 Hz	

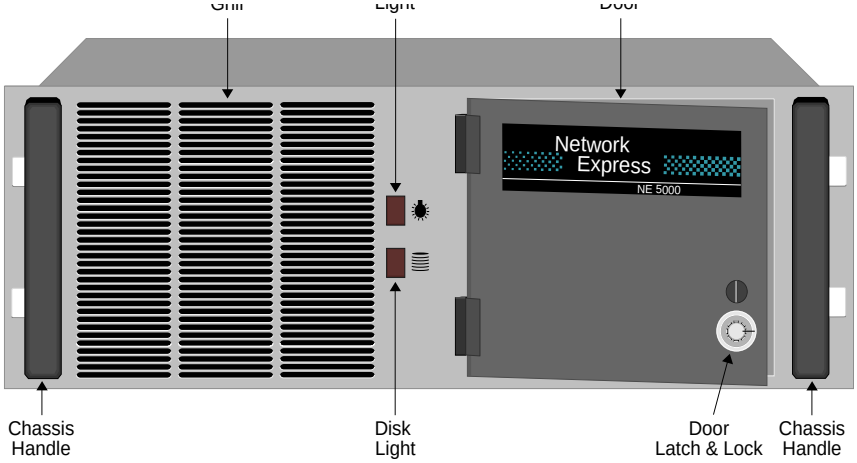
Regulatory Compliance

Meets or exceeds the following:

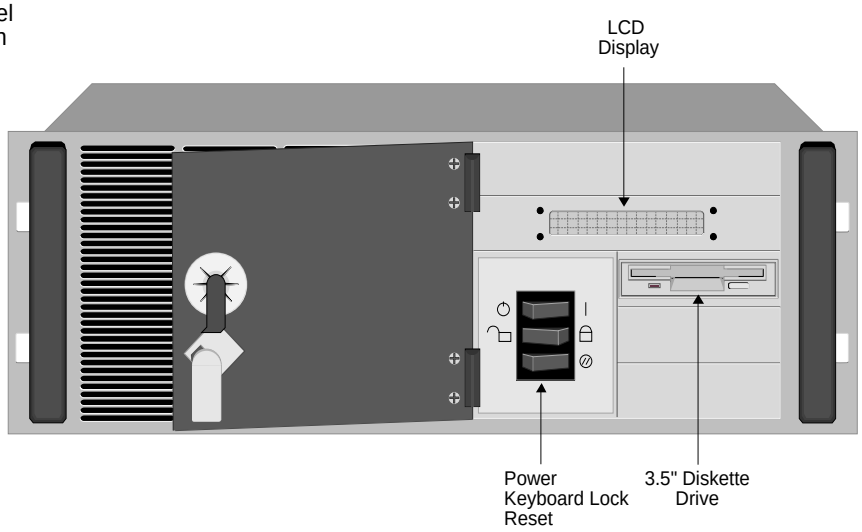
Meets or exceeds the following:

Safety:	UL 1950, CSA C22.2 No. 950, EN 60950, IEC 950, and 72/23/EEC
EMI:	FCC Part 15, EN 55022, CSA 108.8, EN 50082-1, VCCI V-3, and 89/336/EEC

THE NE 5000 PLATFORM (A NETWORK EXPRESS PLATFORM)

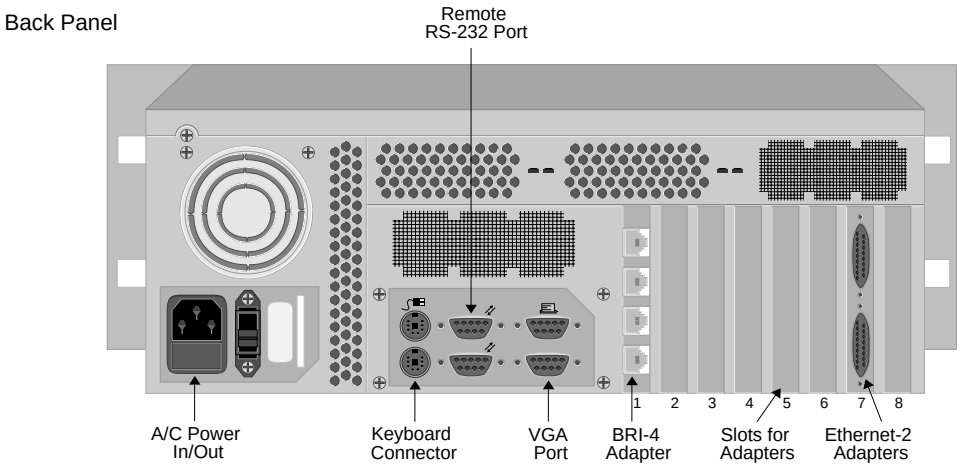


Front Panel
Door Open



PLATFORM DESCRIPTION

The NE 5000 is a rack-mountable platform which provides eight slots for adapters. The front panel has the activity indicators for power-on and disk activity, an air-intake grill, and a peripheral access door, which may be latched or locked closed. Behind the door is located the diskette drive, control buttons, and an LCD display. On the back of the chassis, the rear panel has mountings for a RS-232 serial port, and connectors for a keyboard and a monitor.



CLEANING THE NE 5000 AIR FILTER

The NE 5000 has a removable air filter. This filter is provided to ensure system cleanliness and stability in dusty operating environments. The filter is located just behind the chassis' front panel. For best performance (and as an alternative to replacement) regularly wash the filter in warm water and a mild detergent.

Before removing the air filter for cleaning, read the following warning and caution notes.

WARNING

Before removing the air filter for cleaning, ensure that the system is powered off and the power cord is unplugged from the power source. Note that the Power ON / OFF switch does not disconnect the power from the system. Failure to unplug the power cord can result in serious injury or equipment damage.

CAUTION

An electrostatic discharge (ESD) can damage your system. We recommend that you perform this procedure only at an ESD workstation. If such a workstation is unavailable, provide some ESD protection by wearing an antistatic wrist strap attached to chassis ground when handling components.

To clean the air filter:

1. Power-down the system and disconnect the system's power cord from the power source.
2. Remove the system's top cover.
3. Remove the two retaining screws holding the air filter in place.
4. Tilt the filter toward the rear of the chassis and lift the filter up and out of its position.
5. Once removed, you can clean the filter by washing it in warm water and a mild detergent. Make sure it is completely dry before you place it back in the system.

6. Insert the clean and dry air filter back into its slot behind the chassis front. Tilt the filter forward into place until it is flush against the chassis front panel.

7. Reinstall the two retaining screws along the top lip of the chassis.

8. Replace the system's top cover.

9. Reconnect the power cord and power up the system.

PLATFORM CHARACTERISTICS

Physical Characteristics

Height:	178 mm (7.0 in)
Width:	432 mm (17.0 in)
Depth:	452 mm (17.8 in)
Weight:	22 kg maximum (44 lb. maximum)

Environmental Characteristics

Operating Temp:	0° to 50° C (41° to 122° F)
Operating Humidity:	20 - 85% non-condensing
Operating Altitude:	3048 m maximum (10,000 ft maximum)
Non-operating Shock:	40 G, 11 ms 1/2 sine wave
Storage Temperature:	-25° to +70° C (-13° to 158° F)

Electrical AC Power Input

Voltage:	90 - 135 V	Current:5 A
Voltage:	180 - 265 V	Current:4 A
Frequency:	47 - 63 Hz	

Regulatory Compliance

Meets or exceeds the following:

Safety:	UL 1950, CSA C22.2 No. 950, EN 60950, IEC 950, and 72/23/EEC
EMI:	FCC Part 15, EN 55022, CSA 108.8, EN 50082-1, VCCI V-3, and 89/336/EEC

SYSTEM ADAPTERS

This section describes the following adapters which are supported by Central Site CyberSWITCH platforms:

- Ethernet
- Basic Rate
- Primary Rate
- Expander
- V.35
- RS232
- Digital Modem
- Encryption

For adapter illustrations, refer to the *System Adapters* Appendix. For required adapter settings, refer to the *Hardware Installation* chapter.

ETHERNET ADAPTERS

ETHERNET-2 ADAPTER

The Ethernet-2 adapter was formerly known as the Ethernet adapter.

The Ethernet-2 provides direct support for two Ethernet (or 802.3) LAN connections. In the CyberSWITCH, this adapter provides both local and remote bridging of LAN data.

The Ethernet-2 incorporates an Intel i960 RISC processor executing at 33Mhz. When coupled with the integrated, high-performance Ethernet controllers, the adapter can operate at the maximum speed of the LAN (10Mbps). This is equivalent to a packet rate of 14,800 packets per second (pps).

The adapter has 2MB of DRAM, which allows it to execute sophisticated filtering and forwarding functions. The adapter maintains a large table of over 1000 entries for local MAC addresses.

The front of the adapter has two 15-pin AUI connectors. This provides direct connection for 802.3 transceivers, which accommodates 10Base5, 10Base2, or 10BaseT connectivity.

Hardware Characteristics

Processor:	i960
Speed:	33Mhz
Ports:	2
Port Type:	15pin AUI
MTBF:	75000hours
MTTR:	0.25hour

ETHERNET-1 ADAPTER

The Ethernet-1 adapter was formerly known as the Ethernet LE adapter.

The Ethernet-1 provides direct support for a single Ethernet (or 802.3) LAN connection. In the CyberSWITCH, this adapter provides remote bridging of LAN data.

The Ethernet-1 incorporates an Intel i960 RISC processor executing at 16Mhz. When coupled with the integrated, high-performance Ethernet controller, the adapter can operate at the maximum speed of the LAN (10Mbps). This is equivalent to a packet rate of 14,800 packets per second (pps).

The adapter has 2MB of DRAM, which allows it to execute sophisticated filtering and forwarding functions. The adapter maintains a large table of over 1000 entries for local MAC addresses.

The front of the adapter has a 15-pin AUI connector. This provides direct connection for an 802.3 transceiver, which accommodates 10Base5, 10Base2, or 10BaseT transceiver connections.

HARDWARE CHARACTERISTICS

Processor:	i960
Speed:	16Mhz
Ports:	1
Port Type:	15pin AUI
MTBF:	75000hours
MTTR:	0.25hour

LAN CONNECTION

The CyberSWITCH connects to an Ethernet LAN using a 15-pin AUI connector. A Media Access Unit (MAU) is required for each LAN port. (Note that the MAU is NOT normally included with the CyberSWITCH.) Three options are supported for connection to the Ethernet LAN:

- 10Base5 MAU (Thick Ethernet)
- 10Base2 MAU (Thin Ethernet)
- 10BaseT MAU (Twisted Wire Ethernet)

The MAU's 15-pin connector can directly attach to the Ethernet LAN Adapter, or an AUI cable can be used between the Ethernet LAN Adapter and the MAU. The MAU and AUI cables are NOT normally supplied.

BASIC RATE ADAPTERS

BRI-4 BASIC RATE ADAPTER

The BRI-4 provides four basic rate ports. Each port provides a standard S/T interface for attachment to an ISDN basic rate line. The BRI-4 can take advantage of services such as NTT's INS-64, BOC's Centrex ISDN Basic Rate, or PBX's basic rate lines.

Basic rate is a communications service that provides two 64Kbps B channels for data and a 16Kbps signaling D channel (2B+D). The CyberSWITCH uses the 2 B channels for switched connections to carry device data. Both B channel connections can be active at the same time, to the same or different destinations.

The BRI-4 provides four 4-wire S/T interfaces with separate RJ-45 connectors. It uses external NT1s (when necessary) to connect to the public ISDN. You do not need external ISDN terminal adapters.

In Japan, NTT provides a dedicated service called High Speed Digital-I that uses the same Basic Rate Adapters. This can be either a 64Kb or 128Kbps leased circuit. BRI-4 supports up to four HSD-I circuits.

Hardware Characteristics

Processor:	Intel 80C186
Speed:	16 Mhz
Number of Ports:	4
Connector:	RJ-45
Interface:	Point-to-Point, Point-Multipoint for single device
MTBF:	75000hours
MTTR:	0.25hour

BRI-1 Basic Rate Adapter

The BRI-1 provides a single basic rate port with a standard S / T interface for attachment to an ISDN basic rate line. This adapter can take advantage of such services as NTT's INS-64, BOC's Centrex ISDN Basic Rate and PBX's basic rate lines.

Hardware Characteristics

Processor:	Intel 80C186
Speed:	16 Mhz
Number of Ports:	1
Connector:	RJ-45
Interface:	Point-to-Point, Point-Multipoint for single device
MTBF:	75000hrs
MTTR:	0.25hour

BRI Connection

The BRI adapter uses the four wire S / T ISDN Interface. Each basic rate line will connect to a RJ-45 connector at the back of the system. Refer to the following table which provides the pin and signal assignments for the BRI RJ-45 connector(s).

Pin and Signal Assignment for the BRI RJ-45 Connector(s)

BRI Pin	*Signal*	*Function*
1	NC	No Connect
2	NC	No Connect
3	TX+ to CO	Transmit to Line (T)
4	RX+ from CO	Receive from Line (T)
5	RX- from CO	Receive from Line (R)
6	TX- to CO	Transmit to Line(R)
7	NC	No Connect
8	NC	No Connect

Note: For NTT lines, if the line has a Termination Resistor, remove it from the line jack. These jacks are marked by having their names end in "R" (for example: MJ-8SR or MJ-28SR).

PRIMARY RATE ADAPTERS

Primary Rate is a communications service that provides up to 23 B channels for data and a 64Kbps signaling D channel (for North America and Japan), or up to 30 B channels for data and a 64 Kbps signaling D channel. The system uses the B channels for switched connections to carry device data.

The CyberSWITCH supports the following Primary Rate adapters:

- PRI-8
- PRI-23
- PRI-23 / 30

These adapters are described in the following discussion.

THE PRI-8

The PRI-8 adapter provides a single primary rate port that the CyberSWITCH uses to connect to other CyberSWITCHes. This adapter can take advantage of services such as BOC's and IEC's ISDN primary rate, or NTT's INS-1500.

Using one PRI-8, up to 8 B channel connections can be active at the same time, to the same or different destinations. Up to three expander adapters can be used with one PRI-8 to gain 8 B channel connections per Expander, creating a total of 30 possible connections per line (with one channel is used for a data link). Only two expander adapters are needed for 23 channels. A TDM BUS is used to connect the Expander adapters to the PRI-8.

The PRI-8 provides a 4-wire S / T interface. It uses external Channel Service Units (CSUs) to connect to the public ISDN (when necessary). No external ISDN terminal adapters are needed.

In Japan, NTT provides a dedicated service called High Speed Digital-I that uses the same primary rate adapters. This can be used at rates from 192Kbps to 1536Kbps. The PRI-8 adapter supports up to eight HSD-I circuits.

Hardware Characteristics

Processor:	Intel 80C186
Speed:	16 Mhz
Number of Ports:	1
Connector:	RJ-45
Interface:	Point-to-Point
MTBF:	75000hours
MTTR:	0.25hour

THE PRI-23

The PRI-23 adapter uses an HDLC controller that provides up to 23 HDLC channels on a single adapter. Up to six PRI adapters can be placed in one system.

The PRI-23 adapter provides support for all available data channels on the primary rate interface. Used in North America and Japan where primary rate ISDN runs over T1 framing, it provides support for all 23 available data channels. When used in dedicated line configurations, it supports up to 24 T1 channels.

The PRI-23 adapter is fully compatible with our other WAN adapters and the digital modem. It has both a TDM and an MVIP bus connector to accommodate connection to these adapters.

Note: The PRI-23 adapter was formerly called PRI-23/30 in releases prior to 7.0. *In release 7.0 and beyond*, the name PRI-23 refers to the adapter which supports up to 23 T1 channels *only*. The name PRI-23/30 refers to the adapter which supports up to 23 T1 channels *or* 30 E1 channels.

Hardware Characteristics

Processor:	Intel 80C186
Speed:	16 Mhz
Number of Ports:	1
Connector:	RJ-45
Interface:	Point-to-Point

THE PRI-23/30

Note: On the PRI-23/30 board, switch 8 (S8) on the I/O Switch is not used. The board should function properly with the switch in either ON or OFF position.

The following table defines selected jumpers. Refer to the *Hardware Installation* chapter for specific *jumper settings*.

Jumper	*Usage*
JP1	T1/E1
JP3	T1/E1
JP4	termination
JP6	T1/E1
JP7	termination
JP8	termination
JP9	MVIP
P11	Robbed-Bit Signalling

The PRI-23/30 uses an HDLC controller that provides up to 30 HDLC channels on a single adapter. Up to six PRI-23/30 adapters can be placed in one system.

The PRI-23/30 adapter provides support for all available data channels on the primary rate interface. The PRI-23/30 supports up to 23 T1 channels *or* 30 E1 channels. For dedicated connections, the adapter supports up to 24 T1 channels or 31 E1 channels.

The PRI-23/30 adapter is fully compatible with our other WAN adapters and the digital modem. It has both a TDM and an MVIP bus connector to accommodate connection to these adapters. The PRI-23/30 also provides integrated CSU functionality, so no external CSU is necessary.

Hardware Characteristics

Processor:	Intel 80C186
Speed:	16 Mhz
Number of Ports:	1
Connector:	RJ-45
Interface:	Point-to-Point

PRI-8, PRI-23, AND PRI-23/30 CONNECTION

The Primary Rate adapters use four wire S/T ISDN interface. Each primary rate line will connect to a RJ-45 connector at the back of the system. Refer to the following chart for pin and signal assignments.

Pin and Signal Assignment for the PRI RJ-45 Connector

PRI Pin	*Signal*	*Function*
1	NC	No Connect
2	NC	No Connect
3	TX + to CO	Transmit to Line (T)
4	RX+ from CO	Receive from Line (T)
5	RX- from CO	Receive from Line (R)
6	TX- to CO	Transmit to Line (R)
7	NC	No Connect
8	NC	No Connect

Note: *For the PRI-8 and PRI-23 adapters*: If you connect the CyberSWITCH to a CSU with a different pinout than the CyberSWITCH's PRI pinout described in the above table, you will need a crossover converter between the CyberSWITCH and the CSU.

EXPANDER ADAPTER

The Expander adapter is used with PRI-8s to increase the number of possible connections. Each Expander supports 8 additional connections. Up to three expander adapters can be used with one PRI-8 to gain 8 B channel connections per Expander, creating a total of 30 possible connections per line (with one channel is used for a data link). Only two expander adapters are needed for 23 channels.

HARDWARE CHARACTERISTICS

Processor:	Intel 80C186
Speed:	16 Mhz
MTBF:	75000hours
MTTR:	0.25hour

V.35 ADAPTER

The V.35 adapter provides two V.35 ports. The card contains two female DB26 connectors. A V.35 adapter cable converts the DB26 connection to a standard V.35 connection. You can configure each port for DTE (external clocking) or DCE (internal clocking), and each port supports data rates from 56 Kbps to 2,048 Kbps.

The V.35 supports network side connections, providing dedicated connections to other systems. The adapter can take advantage of network connections such as NTT's HSD-Y lines, DDS lines in the U.S., and private network connections through a T1 multiplexer or a channel bank. The V.35 can also take advantage of switched network connections by using an external Data Service Unit (DSU) or Terminal Adapter. The V.35 supports lead-controlled dialing to the Terminal Adapter.

HARDWARE CHARACTERISTICS

Number of Ports:	2
Connectors:	DB26
Interface:	V.35 DTE or DCE (using V.35 adapter cable)
MTBF:	75000hours
MTTR:	0.25hour

V.35 CONNECTION

The V.35 interface is provided by an adapter cable that converts the DB26 connection on a V.35 adapter to a standard 34-pin V.35 connection.

Each port on a V.35 adapter has software configurable for DTE (external clocking) or DCE (internal clocking). Be sure to use the appropriate V.35 adapter cable (DTE or DCE).

The DTE V.35 adapter cable provides a standard 34-pin connection with male contacts. The DCE V.35 adapter cable provides a standard 34-pin connection with female contacts. The following table shows the pin and signal assignments for the V.35 adapter provided by the adapter cable.

Pin and Signal Assignments for the V.35 Connection

V.35 Pin	*Signal*	*Function*	*V.35 Pin*	*Signal*	*Function*
A	Chass	ChassisGround	V	RXCB	Receive Clock B
B	Gnd	Signal Return	W	NC	No Connect
C	RTS	Request to Send	X	RXCA	Receive Clock
D	CTS	Clear to Send	Y	TXCB	Transmit Clock B
E	DSR	Data Set Ready	Z	NC	No Connect
F	DCD	Data Carrier Detect	AA	TXCA	Transmit Clock A
H	DTR	Data Terminal Ready	BB	NC	No Connect
J	RI	Ring Indicator	CC	NC	No Connect
K	LT	Local Test	DD	NC	No Connect
L	NC	No Connect	EE	NC	No Connect
M	NC	No Connect	FF	NC	No Connect
N	NC	No Connect	HH	NC	No Connect
P	TDB	Transmit Data B	JJ	NC	No Connect
R	RDB	Receive Data B	KK	NC	No Connect
S	TDA	Transmit Data A	LL	NC	No Connect
T	RDA	Receive Data A	MM	NC	No Connect
U	NC	No Connect	NN	NC	No Connect

RS232 ADAPTER

The RS232 adapter provides four RS232 ports. The card contains two female DB26 connectors. An RS232 adapter cable converts the DB26 connection to two standard RS232 connections. Using the RS232 adapter cable, DB26 port #1 becomes RS232 port #1A and port #1B. You can configure each port pair (1A,1B or 2A,2B) for DTE (external clocking) or DCE (internal clocking), and each port supports data rates from 2.4 Kbps to 56 Kbps.

The RS232 supports network side connections, providing dedicated connections to other systems. The adapter can take advantage of slower speed analog lines by using standard synchronous analog modems. The RS232 also supports private network connections through a T1 multiplexer or a channel bank.

HARDWARE CHARACTERISTICS

Number of Ports:	4 (using RS232 adapter cable)
Connectors:	DB26
Interface:	RS232 DTE / DCE (using RS232 adapter cable)
MTBF:	75000hours
MTTR:	0.25hour

RS232 CONNECTION

The RS232 interface is provided by an adapter cable which converts the DB26 connection on a RS232 adapter to two standard 25-pin RS232 connections.

Each port on a RS232 adapter has software configurable for DTE (external clocking) or DCE (internal clocking). Be sure to use the appropriate RS232 adapter cable (DTE or DCE).

The DTE RS232 adapter cable provides two standard 25-pin connections with male contacts. The DCE RS232 adapter cable provides two standard 25-pin connections with female contacts. The following table shows the pin and signal assignments for the RS232 interfaces provided by the adapter cable.

Pin and Signal Assignments for the RS232 Connection

RS232 Pin	*Signal*	*Function*	*RS232 Pin*	*Signal*	*Function*
1	Chass	Chassis Ground	14	NC	No Connect
2	TD	Transmit Data	15	TXC	Transmit Clock
3	RD	Receive Data	16	NC	No Connect
4	RTS	Request to Send	17	RXC	Receive Clock
5	CTS	Clear to Send	18	NC	No Connect
6	DSR	Data Set Ready	19	NC	No Connect
7	Gnd	Signal Return	20	DTR	Data Terminal Ready
8	NC	No Connect	21	NC	No Connect
9	NC	No Connect	22	RI	Ring Indicator
10	NC	No Connect	23	NC	No Connect
11	NC	No Connect	24	NC	No Connect
12	NC	No Connect	25	NC	No Connect
13	NC	No Connect			

DIGITAL MODEMS

The CyberSWITCH supports the DM-8, DM-24, DM-24+ and DM-30+ Digital Modem adapters. These adapters allow the CyberSWITCH to receive calls from asynchronous PPP *remote devices* connected by modem. They also provide a vehicle for *remote analog console* access.

Available Digital Modem adapters include the following type and quantity of modems on a single adapter card:

DM-8	eight V-34+ (33.6 Kbps) modems
DM-24	twenty-four V-34+ (33.6 Kbps) modems
DM-24+	twenty-four K56Flex (56 Kbps) modems
DM-30+	thirty K56Flex (56 Kbps) modems

The Digital Modems support the following remote modem options:

All modem adapters:
- V.34+ (33.6 Kbps)
- V.34 (28.8 Kbps)
- V.32 bis (from 300 bps to 14.4 kbps)
- MN4 (with error control)
- MN5 (with data compression)
- V.42 (with error control and data compression)

DM-24+ and DM-30+ modem adapters only:
- K56Flex (56 Kbps) (firmware may be upgraded to the *ITU V.90* standard)

The number of adapters in a system is limited by the number of ISDN channels and adapter slots available. A maximum of four DM-8s or three DM-24s, DM-24+s, or DM-30+s can be installed and configured at one time. You may combine DM-8s and DM-24s in the same system as long as you do not exceed a maximum of three cards.

Note: Digital Modem adapters are also known as DIG-8 (DM-8), DIG-24 (DM-24), DIG-24+ (DM-24+), and DIG-30+ (DM-30+).

For the DM-24+ and DM-30+, no "+" follows the Digital Modem adapter designation in CFGEDIT. Do not be alarmed; in the case of the DM-24 and DM-24+, the system automatically distinguishes between the two different types of modems.

THE DM-8

Hardware Characteristics

Processor:	LSI LOGIC - LR33000RISC
Speed:	25 Mhz
Number of Ports:	8
Connector:	MVIP
MTBF:	100,000 hours
MTTR:	0.25 hours

THE DM-24

The DM-24 adapter consists of a mother board / daughter board combination. The user-configurable switches on the adapter are located on the back side of the mother board.

Note: "ON" and dip switch numbering ("1","2", etc.) may be labeled on opposite sides of the switch, but the "ON" switch position is always to the right as illustrated in the appendix.

Hardware Characteristics

Processor:	Motorola Power PC
Speed:	25 MHz
Number of Ports:	24
Connector:	MVIP
MTBF:	45,500 hours
MTTR:	.25 hours

THE DM-24+AND DM-30+

The DM-24+ and the DM-30+ adapters consist of a mother board / daughter board combination. The two adapters closely resemble each other; they are distinguishable by the number of modem chips on each of the boards. The DM-30+ with its 30 modems is suitable for E1 (European) trunk lines. The DM-24+ (24 modems) accommodates T1 trunk lines in the US and Japan.

To support the ITU V.90 standard, the DM-24+ and DM-30+ must be of a certain hardware revision level. The adapter's mother board must be REV K or higher; the daughter board must be REV G or higher.

Revision label and pertinent switches are located on the back side of the mother board.

Hardware Characteristics

Processor:	Motorola Power PC
Speed:	25 MHz
Number of Ports:	24 / 30
Connector:	MVIP
MTBF (DM-24+):	45,498 hours
MTBF (DM-30+):	39,105 hours
MTTR:	.25 hours

ENCRYPTION ADAPTER

The CyberSWITCH supports the DES/RSA Encryption adapter. This adapter is available in the United States and Canada only.

The DES/RSA adapter includes a high-speed encryption processor that provides data encryption capabilities to the CyberSWITCH. This processor has been implemented in a hardware LSI chip and designed into an ISA bus board and a PCMCIA card. The adapter is a "stand-alone" adapter; it plugs into any CyberSWITCH slot, needing no lines, cables or connectors.

Only one encryption adapter may be installed and configured per CyberSWITCH system.

HARDWARE CHARACTERISTICS

MTBF:	100,000 hours
MTTR:	0.25 hour

SOFTWARE OVERVIEW

OVERVIEW

The system software fits into one of three categories:

- system software for the System, adapter modules and administration functions
- administration software that provides configuration, diagnostics and maintenance on the CyberSWITCH
- system files containing configuration and operational information

This chapter provides an overview for each of the above software categories.

SYSTEM SOFTWARE

Included with each CyberSWITCH is a set of 3.5" high-density diskettes which contain system software, administration software and all required system files. The system software is a set of executable programs that collectively implement the system functions. These programs provide the core interoperability hub features, such as centralized management and high speed digital connections. Depending on the software version purchased, it supports up to eight, sixteen, thirty-two, or forty-eight connections.

Instructions for installing new system software and for upgrading existing system software can be found in the *Upgrading System Software* chapter.

ADMINISTRATION SOFTWARE

A CyberSWITCH may be configured as an SNMP Agent. An SNMP Manager, such as Cabletron's *Spectrum* product, may use these SNMP Agents to monitor individual network devices' operating statistics and configuration elements. The software for this feature is included with the system software.

Carbon Copy, a communications package from Microcom Corporation, is included with the system software. Carbon Copy allows access to all administration functions through the remote administration port on the CyberSWITCH. The CyberSWITCH is configured for 9600 bps direct connect for Carbon Copy remote access. This modem configuration setting may be changed if necessary. Refer to the *Carbon Copy* section in the *Remote Management* chapter for instructions on changing modem configuration settings.

The Manager (Administration Services), is a separate diskette available as an option when you order your system. This diskette contains the Carbon Copy "Guest" software to access the remote administration console option.

SYSTEM FILES

The system files consist of the required configuration files, as well as the operational files that the CyberSWITCH maintains. All of these files may be accessed by using available administrative commands. (Refer to the *System Commands* chapter for details.)

Below is a brief description of the configuration and operational files.

CONFIGURATION FILES

The configuration files store the configuration data. These files are located in the system's `\config` directory. You can maintain these files by using the CFGEDIT configuration utility, which is delivered with the system. You can also make changes to these files through Manage Mode.

The configuration files associated with the system are:

`network.nei`
This configuration file contains information about the switched network.

`devdb.nei`
This file contains the On-node Device Database configuration information about each remote device.

`node.nei`
This configuration file contains node-specific information like resources, lines, CyberSWITCH operating mode and security options, along with the Throughput Monitor Configuration information. If enabled, SNMP configuration information is also in this file.

`lan.nei`
This file contains configuration information used when the bridge is enabled. This file also contains information for the Spanning Tree protocol used for the bridge. Information from this file is configured and used only when the bridge is enabled.

`ip.nei`
This file contains configuration information used when the IP routing is enabled. This file also contains information regarding network interfaces, RIP, and static routes. Information from this file is configured and used only when the IP routing is enabled.

`ipx.nei`
This file contains configuration information used when the IPX routing is enabled. This file also contains information regarding network interfaces, RIP, and static routes. Information from this file is configured and used only when the IPX routing is enabled.

`filter.nei`
This file contains all filter configuration information (bridge, hardware, and IP). This file is new to Release 7.2 software, but is compatible with previous software versions, which contained filter information in the `lan.nei` and/or `ip.nei` files. With Release 7.2 configuration changes and configuration file updates, this filter information will be moved to `filter.nei`.

`atalk.nei`
This file contains configuration information used when AppleTalk Routing is enabled. This file also contains information regarding ports and static routes. Information from this file is configured and used only when the AppleTalk routing is enabled.

`platform.nei`
This is a text file that contains a list of platform names and the currently selected platform. Each line in the file contains an ASCII string representing a platform name and a corresponding integer value. The integer value is the crucial item, since this is what the system software uses to determine whether any special action is necessary. The string is displayed when the *ver* command is issued.

`sdconf.rec`
This is not a system file; it is a configuration file delivered on the ACE Server. However, you may TFTP this file to the system's `\config` directory as an alternate method of providing the system with ACE Server configuration information.

OPERATIONAL FILES

While the CyberSWITCH is running, it collects system statistics and logs system messages. The system maintains these statistics and messages in separate memory-resident tables. The ten most recent versions of each table are available on the system disk.

You can retrieve and view the current memory-resident tables at any time by using the following console commands:

dr	This command will display system messages.
da	This command will display authentication messages.
ds	This command will display system statistics.

You can write the tables to disk by using the following commands:

wr	This command will write the current system messages to disk.
wa	This command will write the current system messages to disk.
ws	This command will write the current system statistics to disk.

Note: When the system is shut down, the tables are automatically written to disk.

The system stores the tables in ASCII format files on the System disk. When the system writes system messages to disk, it stores them in the following location:

Directory: `\log`
File Name: `rprt_log.nn`
Where "nn" is an integer that is incremented each time a new file is written.

When the system writes system statistics to disk, it stores them in the following locations:

Directory: `\log`
File Name: `stat_log.nn`
Where "nn" is an integer that is incremented each time a new file is written.

USER LEVEL SECURITY FILES

As administrator, you may create a welcome banner file as well as a message-of-the-day file to display at login with user level security. Neither file should exceed the limits of 80 characters in width and 21 lines in length, and must reside in the `\config` directory. The creation of these files is optional; if you choose to use them, create the files, and TFTP them to the CyberSWITCH.

`welcome.nei`
This file contains the text of the administrator-defined welcome banner. It is displayed when a user initiates a network login.

`motd.nei`
This file contains the text for the administrator-defined message of the day. It is displayed when the user is validated after log-in.

SYSTEM INSTALLATION

We include the following chapters in this segment of the *User's Guide*:

- *Ordering ISDN Service*
  Provides guidelines for ordering ISDN service in the United States.

- *Hardware Installation*
  Step-by-step instructions for installing hardware components.

- *Accessing the CyberSWITCH*
  Provides a description of the possible ways to access the CyberSWITCH (for diagnostic purposes or for software upgrades).

- *Upgrading System Software*
  A description of the software upgrade process.

ORDERING ISDN SERVICE (US ONLY)

OVERVIEW

This chapter was designed to be a guideline for ordering ISDN service in the United States.

For BRI ISDN Service:
If you are using NI-1 lines, try using EZ-ISDN Codes to order BRI service. If your service provider does not support EZ-ISDN Codes, try using the NI-1 ISDN Ordering Codes.

If your service providers does not support either types of codes, or, if you are using a non-NI-1 line, refer to *Ordering BRI ISDN Lines using Provisioning Information*.

For PRI ISDN Service:
If you are using PRI lines, refer to *Ordering PRI ISDN Lines*.

ORDERING NI-1 LINES USING EZ-ISDN CODES

If you are using a NI-1 switch type and your service provider supports EZ-ISDN codes, we recommend using the EZ-ISDN 1 code. EZ-ISDN 1 provides alternate circuit-switched voice / data on both B-Channels. There is a CSV / D terminal associated with each of the B-channels.

The B-channels will be given a unique primary directory number capable of making / receiving one circuit-switched voice or circuit-switched data call. Additionally, calling line Id is also supported.

ORDERING NI-1 LINES USING NI-1 ISDN ORDERING CODES

If you are using a NI-1 switch type and your service provider supports ordering codes, we recommend NI-1 ISDN Capability Package I. This package includes circuit-switched data on two B channels. Data capabilities include Calling Line Id. No voice capabilities are provided. The lack of voice feature may save you money. However, package K or M will also work.

ORDERING BRI ISDN LINES USING PROVISIONING SETTINGS

If your service provider does *not* support EZ-ISDN or ISDN Ordering Codes, or you are using a non-NI-1 line, use this section when ordering your BRI ISDN line.

When the phone company installs the line, they assign it certain characteristics. These are different depending on the type of ISDN switch to which the line is attached. AT&T's 5ESS NI-1 and Northern Telecom's DMS100 NI-1 are among the most popular.

When ordering an ISDN line, there are general steps to follow that apply to all types, and there are steps specific to your line type. The general steps to follow are:

1. Contact your service provider to determine the type of available switch.

2. Ask your service provider for the available types of ISDN services.

If the AT&T 5ESS switch type is available, the ISDN services available will be one of the following:
- NI-1
- Custom Point-to-Point

If Northern Telecom DMS-100 switch type is available, the ISDN services available will be one of the following:
- NI-1
- DMS-100 Custom

3. Refer to section in this document that applies to your service type.

4. Order your ISDN service. If available, ask for two telephone numbers and two *SPIDs* for your ISDN line.

5. If necessary, provide your service provider with the appropriate provisioning settings in this document.

6. After installation, make sure you have the following information:
   - switch type
   - telephone numbers
   - SPIDs

The following sections provide provisioning settings for your specific service type.

PROVISIONING SETTINGS FOR AT&T 5ESS SWITCHES

The ISDN services supported by AT&T 5ESS switches are as follows (in order of preference of usage):

1. NI-1

2. AT&T Custom Point-to-Point

The sections below provide the settings for each 5ESS service type. Note that your service provider may not be able to offer all of the features listed.

AT&T 5ESS NI-1 SERVICE

Note that some of the elements below are set per directory number. With NI-1 Service, you will typically have two directory numbers.

AT&T #5ESS NI-1 Service	
Provisioning Element	*Setting*
Term Type	A
CSV	1
CSV ACO	unrestricted
CSV limit	2
CSV NB limit	1
CSD	1
CSD ACO	unrestricted
CSD limit	2
CSD NB limit	1
EKTS	no
ACO	yes

AT&T 5ESS Custom Point-to-Point Service

Note that some of the elements below are set per directory number. With Custom Point-to-Point Service, you will have two directory numbers.

AT&T Custom Point-to-Point Service	
Provisioning Element	*Setting*
Term Type	E
CA	1
CA quantity	1
CSV	0
CSV CHL	no
CSV limit	2
CSD	2
CSD CHL	any
CSD limit	2
DSL CLS	PP

Provision Settings for Northern Telecom DMS-100 Switches

The ISDN services supported by Northern Telecom DMS-100 switches are as follows (in order of preference of usage):

1. NI-1

2. Custom Service

The sections below provide the settings for each DMS-100 service type. Note that your service provider may not be able to offer all of the features listed.

NORTHERN TELECOM DMS100 NI-1 SERVICE

Note that you must set either EKTS or ACO to yes. You may not set both of them to yes.

Northern Telecom DMS100 NI-1 Service	
Provisioning Element	*Setting*
signaling	functional
PVC	2
TEI assignment	dynamic
maxkeys	3 is preferable 1-64 is acceptable
release key	no
ringing indicator	no
EKTS	no
ACO	yes
number of call appearances	2 is standard number may vary depending on voice features ordered
notification busy limit	1 (always one less than number of call appearances)
LCC	ISDNKSET

NORTHERN TELECOM DMS100 CUSTOM SERVICE

Note that you must set either EKTS or ACO to yes. You may not set both of them to yes.

Northern Telecom DMS100 Custom Service	
Provisioning Element	*Setting*
signaling	functional
PVC	1
TEI assignment	dynamic
maxkeys	3 is preferable 1-64 is acceptable
release key	no
ringing indicator	no
EKTS	no
ACO	yes
number of call appearances	2
LCC	ISDNKSET
version	functional
CS	yes
PS	no

BASIC INFORMATION FOR ORDERING PRI ISDN LINES

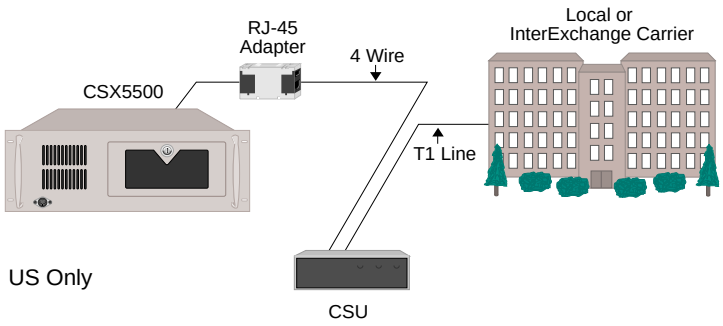
ISDN Primary Rate is a communications service that allows the system to make up to 23 connections over a single line. It uses a 4-wire T1 line that carries 24 channels, each providing 64000 bps bandwidth. The service uses channels 1 to 23 as bearer (B) channels to carry connections between two systems. The 24th channel is used for signaling information (the data link).

The customer should request the following options for a Primary Rate Line that is connected directly to a CyberSWITCH:

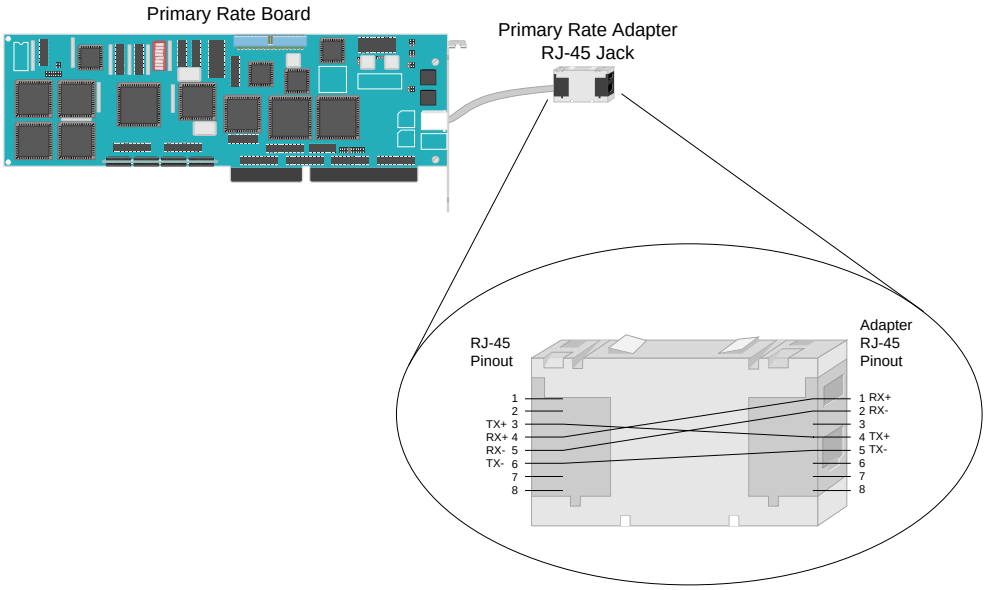
- B8ZS encoding
- ESF framing
- all channels should be Circuit Switched Data
- Hunt Group (if desired)
- call bandwidth supported (56Kbps, 64Kbps, and / or 384Kbps)
- CLID (calling line Id); usually there is no charge for this

In order to connect to the Primary Rate line, the customer must provide a Channel Service Unit (CSU). If the line is provided by a LEC or IXC, the CSU is required by the phone company to protect the phone network from any problems with customer premise equipment. At the time that the line

is ordered, the customer may be asked for the FCC registration number for the type of CSU that is being used. The CSU should support ESF framing and B8ZS line encoding.



The cabling between the CSU and the CyberSWITCH is very important, and is also where most problems occur. The system's PRI RJ-45 adapter uses the international standard of pins 3, 4, 5, and 6 for transmit and receive. Most T1 lines in the United States use the traditional 1, 2, 4, and 5 pins. We provide an RJ-45 to RJ-45 Adapter that will convert between the two wiring systems. The customer may still need a special cable to connect from a RJ-45 jack to a DB-15 connector, if that is what the CSU provides.



Otherwise, a standard 4 or 8 wire cable with RJ-45 jacks is sufficient between the Adapter and the CSU.

When the line is installed, the customer must ask the phone company the following questions:

1. What are the phone numbers for the line? (There may be more than one.)

2. Do I need to use any prefix when I dial? (For example, "9" for a Centrex line.)

3. What type of switch is the line connected to?

4. For #4ESS, what release of software is running on the switch?

When the phone company installs the line, they assign it certain characteristics (sometimes called translations). These are different depending on the type of ISDN switch to which the line is attached. The customer must know what type of switch is being used.

The following table provides correct settings for important configuration options.

Option	*Local Bell Operating Company*		*AT&T Network*	*U.S. Sprint & MCI*
Type of Switch	#5ESS	DMS100	#4ESS	DMS250
Encoding	B8ZS	B8ZS	B8ZS	B8ZS
Framing	ESF	ESF	ESF	ESF
Network Facilities	NA	NA	SDS or Call-By-Call	NA
Echo Cancellation	NA	NA	NA	OFF (Disabled)

HARDWARE INSTALLATION

OVERVIEW

This chapter provides a description of the hardware installation process. It includes:

- *pre-installation requirements*
- *selecting slots for adapters*
- *setting switches*
- *inserting adapters into backplane*
- *connecting inter-board cables*

Your distributor may have already completed this adapter installation. If not, follow this chapter's specific instructions.

Only qualified personnel should install adapters into the CyberSWITCH.

Any time you remove the system module cover, unplug the power cord. Failure to do so may result in personal injury or equipment damage.

The CyberSWITCH is sensitive to static discharges. Use a grounding strap and observe all static precautions during this procedure. Failure to do so could result in damage to the CyberSWITCH.

PRE-INSTALLATION REQUIREMENTS

Before you begin the installation process, be sure to:

- *Choose a suitable setup location*
  Make sure the location is dry, ventilated, dust free, static free, and free from corrosive chemicals

- *Verify system power requirements*
  If applicable, make sure the line voltage select switch is set for the AC input power source you are going to use. The appropriate standard power cord is supplied with the system.

  CAUTION:
  When changing the line voltage select switch, make sure the AC power cord is unplugged.

- *Verify cabling requirements*
  The cabling included with your shipment will depend on the country in which your system will operate. If additional cabling is needed other than what was shipped, contact your distributor.

- *Verify administration console requirements*
  You will need an administration console to install your system. (We do not provide this.) The system supports two administration console options: a local administration console in which a keyboard and monitor are directly connected to the system, or a remote administration console in which an IBM Compatible PC is remotely connected to the system. Refer to *Accessing the CyberSWITCH* for more details.

- *Provide a diskette for configuration backup*
  If you choose to back up your configuration to diskette (as opposed to a Network Management Station), you will need a 3 1/2" DOS formatted high-density diskette. Details on performing a configuration backup are described in the *Routine Maintenance* chapter.

SELECTING SLOTS FOR THE ADAPTERS

Most adapter settings are dependent upon the slot in which the adapter will be installed and/or configured. So, to determine each adapter's settings, you must first select the proper slot for each adapter. As you select the slot for each adapter, note the slot number you plan to associate with each adapter. You will need this information for the next step: *Adapter Settings.*

Throughout this section, we refer to LAN, WAN, DM (Digital Modem), and Encryption adapters. The following chart lists the adapters in each group.

Adapter Group:	LAN	WAN	DM	Encryption
Adapters:	Ethernet-1 Ethernet-2	BRI-1 BRI-4 PRI-8 PRI-23 PRI-23/30 RS232 V.35	DM-8 DM-24 DM-24+ DM-30+	DES/RSA (USA)

A CyberSWITCH supports a maximum of one LAN, one Encryption, and up to six "other" adapters (WAN+DM). Of this total of six, a maximum of 4 DM-8s or 3 DM-24s, DM-24+s or DM-30+s are allowed. Refer to the *Hardware Overview* for any additional restrictions that may be platform-specific.

The following steps determine each adapter's slot placement. Note that all WAN, DM, and Encryption adapters fall between the CPU and the LAN in the backplane.

1. Select a WAN adapter for the first slot adjacent to the CPU. Then continue as follows:

   a. *If you are installing only WAN adapters:*
   Continue to select WAN adapters for the next available slots until you have selected a slot for all WAN adapters.

   b. *If you are installing WAN adapters and DM adapters:*
   Select a DM adapter for the next available slot. Continue alternating WAN and DM adapters until you run out of WAN or DM cards. At this point, continue with the remaining WAN or DM adapters until you have selected a slot for all remaining WAN or DM adapters.

c. *If you are installing WAN adapters and an Encryption adapter:*
Select slots for all WAN adapters as described in *step a*, then select the next available slot for the Encryption adapter.

d. *If you are installing WAN and DM adapters, and an Encryption adapter:*
Select slots for all WAN and DM adapters as described in *step b*, then select the next available slot for the Encryption adapter.

2. Finally, select a slot for the LAN adapter, leaving an empty slot between the LAN adapter and the other adapters, if possible.

ADAPTER SETTINGS

Adapter settings fall into the following groups:

- *adapter interrupt and I/O address settings*, which are slot-number dependent
- *MVIP termination settings* to properly terminate the MVIP bus
- *Encryption adapter settings*
- *additional adapter settings*, which are specific to the PRI adapters

ADAPTER INTERRUPT AND I/O ADDRESS SETTINGS

WAN ADAPTERS

The WAN adapters (except for the RS-232 and V.35) use jumpers to set the interrupt and switches to set the I/O address. The following chart contains the WAN adapter's interrupt jumper and I/O address switch settings required for each configured slot number.

Configured Slot	*Interrupt Jumper (Interrupt Block)*	*I/O Address Switch Setting (SW1)*
1	Position 3	Value 340 S1, S2, S3, S4, S5, S6, S7, S8 on, on, on, off, on, off, off, off
2	Position 11	Value 348 S1, S2, S3, S4, S5, S6, S7, S8 off, on, on, off, on, off, off, off
3	Position 5	Value 350 S1, S2, S3, S4, S5, S6, S7, S8 on, off, on, off, on, off, off, off
4	Position 10	Value 358 S1, S2, S3, S4, S5, S6, S7, S8 off, off, on, off, on, off, off, off
5	Position 7	Value 360 S1, S2, S3, S4, S5, S6, S7, S8 on, on, off, off, on, off, off, off
6	Position 12	Value 368 S1, S2, S3, S4, S5, S6, S7, S8 off, on, off, off, on, off, off, off

Refer to the *System Adapters Appendix* for location and numbering conventions of the interrupt block and I/O switch. Note the following:

- *concerning the interrupt block*: On some boards, such as the PRI-8, the interrupt block is numbered from left to right, beginning with position 3 on the left. On the PRI-23 and PRI-23/30, the interrupt block is numbered from right to left, with position 3 starting on the right.
- *concerning the I/O Switch*: If the adapter's I/O address switches are labeled with *open* as opposed to either *off* or *on*, open corresponds to *off*. On the PRI-23/30, S8 on the I/O Switch is not used. The board should function properly with the switch in either the ON or OFF position.

DM-8 ADAPTER I/O ADDRESS SETTINGS

The DM-8 is unique in that it has no interrupts, and uses jumpers instead of switches for its I/O address settings. The DM-8 will take on the interrupt of the slot in which it is configured. You only need to set its I/O address. When configuring DM-8 adapters, use 380 for the I/O address of the

first DM-8 installed, 388 for the second, 390 for the third, and 398 for the fourth. Refer to the *System Adapter Appendix* for jumper locations; refer to the following chart for the required jumper settings.

DM-8 Adapter (Address)	*I/O Address Jumper Settings*
1st adapter (address 380)	J2, J3, J4 on, on, on
2nd adapter (address 388)	J2, J3, J4 off, on, on
3rd adapter (address 390)	J2, J3, J4 on, off, on
4th adapter (address 398)	J2, J3, J4 off, off, on

Note: When the table says *on* for a certain pair of prongs (J2, J3, or J4), it means that a jumper needs to be in place for that pair. *Off* indicates that no jumper is needed for that pair.

DM-24 ADAPTER INTERRUPT AND I/O ADDRESS SETTINGS

The DM-24 adapter uses switches to set the interrupt and I/O address. Since the DM-24's only available interrupts are 10, 11, and 12, and these interrupts are associated with configured slots 2, 4, and 6, these are the only slots available for these cards. Refer to the *System Adapter Appendix* for switch locations; refer to the following chart for switch settings.

Configured Slots	*Interrupt Switch (IRQ) S2*	*I/O Address Switch Setting S3*
2	IRQ = 11 1, 2, 3, 4, 5, 6 off, off, off, off, on, off	Address: 300 1, 2, 3, 4, 5, 6 A4, A5, A6, A7, A8, A9 on, on, on, on, off, off
4	IRQ = 10 1, 2, 3, 4, 5, 6 off, off, off, off, off, on	Address: 310 1, 2, 3, 4, 5, 6 A4, A5, A6, A7, A8, A9 off, on, on, on, off, off
6	IRQ = 12 1, 2, 3, 4, 5, 6 off, off, off, on, off, off	Address: 320 1, 2, 3, 4, 5, 6 A4, A5, A6, A7, A8, A9 on, off, on, on, off, off

Note: The silk screening may vary from card to card. If your card uses the labeling DIS/EN or =1/=0, note the following: For IRQ, "off" is the same as DIS (disabled); "on" is the same as EN (enabled). For I/O address, "off' is the same as "1"; "on" is the same as "0".

DM-24+ AND THE DM-30+ ADAPTER ADDRESS SETTINGS

The DM-24+ and the DM-30+ adapters both use switches to set the interrupt, I/O address, and MVIP clock termination. Switch blocks SW1 and SW3 determine I/O address, SW2 and SW4 determine interrupts, and SW5 determines MVIP clock termination.

Note: Refer to the *System Adapter Appendix* for switch locations. Configure a DM-24+ or a DM-30+ *only* in slots 2, 4, and / or 6. Switch settings will differ depending upon the slot you wish to configure. Refer to the following charts / descriptions:

Configured Slots	***Interrupt Switches (IRQ on) SW2***	***Address***
2	IRQ=11	300
4	IRQ=10	310
6	IRQ=12	320

To set the IRQ so that it is on, refer to switch blocks SW2 and SW4. Set the corresponding IR switch on these switch blocks to on, with all others off. For example, for an IRQ setting of 11, IR11 (switch 4) on switch block SW2 should be *on*; all other IR switches on SW2 and SW4 should be *off*.

To set the address, refer to switch blocks SW1 and SW3. SW1 is labeled 1 through 8 (A15 through A8). Switches in this block should always remain *on*, *on*, *on*, *on*, *on*, *on*, *off*, *off*. SW3 varies based on address. Use the following chart:

Address	***Switch***	***Settings***			
300	SW3	1	2	3	4
		A7	A6	A5	A4
		on	on	on	on
310	SW3	1	2	3	4
		A7	A6	A5	A4
		on	on	on	off
320	SW3	1	2	3	4
		A7	A6	A5	A4
		on	on	off	on

For example, for an address of 300, A9 (switch 7) and A8 (switch 8) on SW1 should be *off*; all remaining switches on SW1 and SW3 should be *on*.

Note: For all configurations, switch 4 on SW4 is a reserved switch and must always remain OFF.

ENCRYPTION ADAPTER SETTINGS

DES/RSA Adapter

The DES/RSA adapter is available in the United States and Canada only. The adapter has a set of eight dip switches in a switch block labelled SW1. Set these dip switches to map the encryption adapter memory at D800:

SW1 Memory Mapped Address	1	2	3	4	5	6	7	8
D800	OFF	OFF	OFF	OFF	OFF	OFF	OFF	ON

The adapter has one jumper (J1), which *must be installed*!

MVIP SETTINGS

The following adapters have MVIP connectors:

- PRI-23,
- PRI-23/30,
- DM-8,
- DM-24,
- DM-24+, and
- DM-30+

In order to establish an MVIP bus, follow this process:

1. First, select slots for all MVIP adapters. If you are using both PRI and DM adapters, begin with a PRI adapter, and then select slots alternating PRI and DM adapters as described in *Selecting Slots for Adapters*.

2. Next, *terminate the MVIP jumpers* on both the *first and last adapter* in the MVIP adapter series. (All other MVIP jumpers on the adapters between these two should be left unterminated).
   - To terminate the MVIP bus for the *PRI-23*, place the jumpers vertically on JP9.
   - To terminate the MVIP bus for the *PRI-23/30*, place the jumpers vertically on JP9.
   - To terminate the MVIP bus for the *DM-8*, place jumpers horizontally on J5 and J6.
   - To terminate the MVIP bus for the *DM-24*, turn switch blocks S1 and S4 "ON".
     Note: DM-24 adapters may have either toggle or slide switches. In either case, the switch is "ON" if it is toggled or slid to the right. All four switches should always be set in the same direction.
   - To terminate the MVIP bus for the *DM-24+* or the *DM-30+*, place the four switches in switch block SW5 to the "ON" position.

3. Install MVIP adapters into pre-selected slots.
4. Install MVIP ribbon cable. *Refer to Connecting Adapter Inter-board Cables*.
5. Install TDM ribbon cable. *Refer to Connecting Adapter Inter-board Cables*

In order to improve signal quality (which in turn results in higher modem-connection rates), you should terminate the MVIP bus at both ends as recommended in step (2). However, not all system configurations support this. Note that PRI-8, PRI Expansion and BRI boards do *not* support MVIP termination.

Note: MVIP termination at both ends (step 2) also applies to six PRI-23/30 configurations.

ADDITIONAL ADAPTER SETTINGS

On certain adapters, there are specific jumper settings which are independent of slot configuration. These adapters include the:

- PRI-8
- PRI-23
- PRI-23 / 30

Refer to the *System Adapters Appendix* for the locations of various jumpers.

PRI-8

Line Type Settings

In addition to the interrupt jumper and I/O address settings, the PRI-8 has settings specific to the PRI line type in use. Refer to the following table for correct settings. Place the jumper on the pins identified to enable the function.

PRI Line Type	*J20 Clock*	*J11 Clock*	*J12, J13 Receive Pair*	*J14, J15 Transmit Pair*
T1	Bottom	Right	Bottom Pair	Left Pair
E1 75 ohms	Top	Left	Middle Pair	Middle Pair
E1 120 ohms	Top	Left	Top Pair	Right Pair

PRI-23

Clock Settings

In addition to the interrupt jumper and I/O address settings, the PRI-23 requires clock settings (JP4 through JP7). Refer to the following table for the correct settings. Place the jumper on the pins identified to enable the function.

Jumper	*Jumper Setting North American and Japan T1*
J6	1-2
J7	1-2
J8	1-2
J9	1-2
J10	1-2
J11	1-2
J12	1-2
J13	1-2
J14	1-2
JP2	3-4
JP3	3-4
JP4	1-2
JP5	1-2
JP6	1-2
JP7	1-2

PRI-23/30

In addition to the interrupt jumper and I/O address settings, the PRI-23/30 requires settings for:

- channel selection (T1 or E1)
- MVIP bus termination
- Robbed Bit Signaling (RBS)
- E1/R2 signaling

Refer to the following chart for correct settings. Place the jumper on the pins identified to enable the function, unless specified otherwise.

Jumper	Function	T1 (short haul) 100 ohms TP	T1 (long haul) 100 ohms TP	E1 (short haul) 75 ohms coax	E1 (short haul) 120 ohms TP	E1 (long haul) 120 ohms TP
JP1	T1/E1	2-4	2-4	1-3	1-3	1-3
JP3	T1/E1	3-4	3-4	1-2	1-2	1-2
JP4**	termination**	1-2	1-2	3-4	5-6	5-6
JP6	T1/E1	jumper in	jumper in	no jumpers	no jumpers	no jumpers
JP7**	termination**	1-2	1-2	1-2	1-2	2-3
JP8**	termination**	1-2	1-2	1-2	1-2	2-3
JP9	MVIP	jumper in to terminate	jumper in to terminate	jumper in to terminate	jumper in to terminate	jumper in to terminate
JP11*	RBS* R2 signaling (Korea)	jumper out to enable N/A	jumper out to enable N/A	N/A jumper out to enable	N/A jumper out to enable	N/A jumper out to enable

Note: When setting jumpers, orient the adapter so that the bus connectors are at the top of the adapter, and all pin numbers are in an upright position.

Note that JP1 has an unusual pin-numbering scheme. Be sure to place jumpers vertically (on pins 1 and 3 or pins 2 and 4, depending upon channel selection). The only jumper that you will need to place horizontally is JP4.

* T1 mode supports RBS functionality; E1 mode supports R2 functionality. Use JP1, JP3 and JP6 to designate either T1 or E1 mode.

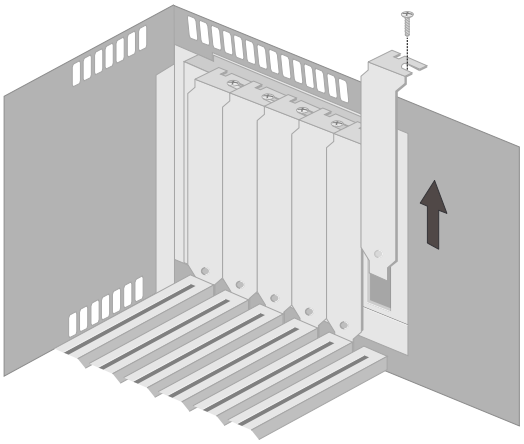
** Refer to *Termination Guidelines*.

INSERTING THE ADAPTERS INTO THE CYBERSWITCH

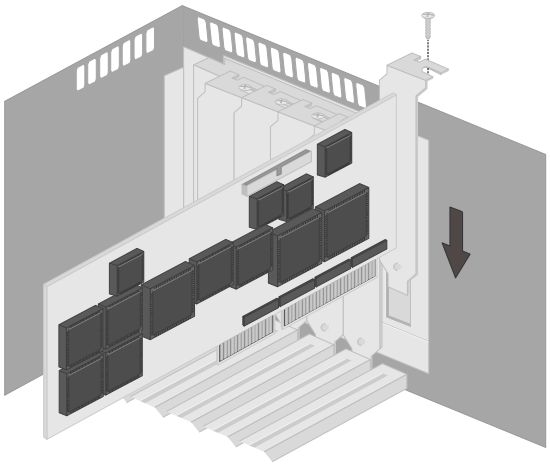
Now that you've selected the slots and set all switches and jumpers, insert the cards in this way:

1. Remove any existing board hold-down bars / brackets to obtain clear access to the backplane ISA bus connectors.

2. Remove the adapter hold-down screw located on the bracket of the appropriate slot, and remove the bracket. This screw will be needed later to secure the adapter once in place.



3. Holding the adapter by the edges only, slide the adapter into the appropriate slot. Use the adapter guide to align the adapter into place.



4. Once the adapter's gold contacts are lined up with the slots they fit into, use your thumbs to apply pressure to the outer edge of the adapter to gently push the contacts into place.

5. Reinsert the adapter hold-down screw.

CONNECTING ADAPTER INTER-BOARD CABLES

There are three possible cables used to connect adapters: flat, crossover, and LCD. Flat cables connect adapters with like connectors, and crossover cables connect the flat cables of adapters with differing connectors. LCD cables apply to former Network Express products (NE2000-II, 4000, 5000) only. These cables connect the system's liquid crystal display (LCD) to the WAN adapter group.

CONNECTING MULTIPLE ADAPTERS

WAN and DM adapters need inter-board cables to communicate with each other over an inter-board bus. (LAN, V.35, RS232 and encryption adapters never require inter-board cabling.) The WAN adapters use either a Time Domain Multiplexing (TDM) bus, a Multiple Vendor Integration Protocol (MVIP) bus, or both. The DM adapters use an MVIP bus only. Each adapter has at least one bus connector, and some (such as the PRI-23 and PRI-23/30) have both.

The following table classifies the adapters according to inter-board connector type:

Adapter	*Inter-Board Connector Type*
LAN (Ethernet)	(none)
V.35	(none)
RS232	(none)
BRI-1	(none)
BRI-4	TDM
PRI-8	TDM
PRI-23	both TDM and MVIP
PRI-23/30	both TDM and MVIP
Expander	TDM
DM-8	MVIP
DM-24	MVIP
DM-24+/30+	MVIP
encryption (DES/RSA)	(none)

All TDM and MVIP connectors, if present, are along the top of the card as shown in the *System Adapters Appendix*. If you are unsure of the location of the adapter's connectors, refer to the adapter illustrations for clarification.

The type of inter-board bus (or buses) you should install depends upon your unique system configuration. The following suggestions should help you achieve the cleanest connections:

If you have PRI-23/30 cards: Use an MVIP bus connection between cards whenever possible to achieve the best results. This applies to both:

- multiple PRI-23/30 configurations
- PRI-23/30 cards in combination with DM cards

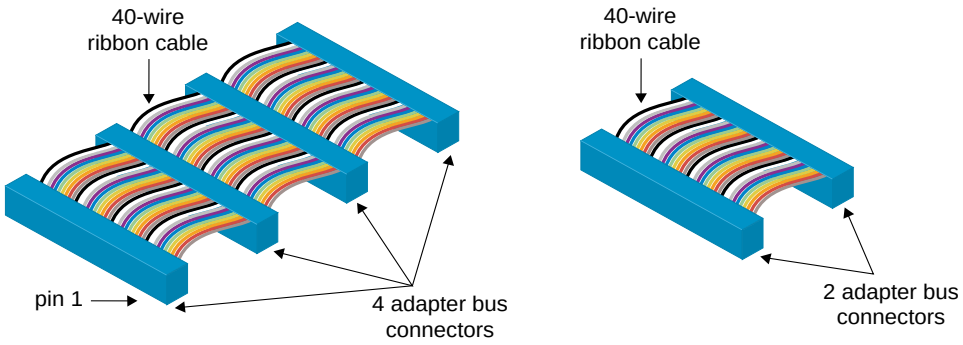
If you have only PRI-23 cards: Use a TDM bus between WAN cards and an MVIP bus to connect to the DM. (I.e., connect *all* TDM connectors to other TDM connectors, and *all* MVIP connectors to other MVIP connectors within the system.)

If you have a mixture of PRI-23 cards and PRI-23/30 cards: Use both a TDM bus and an MVIP bus. Connect *all* TDM connectors to other TDM connectors, and *all* MVIP connectors to other MVIP connectors within the system.

If you have BRI, PRI-8 or Expander cards: You must use a TDM bus. If you also have a DM card in your configuration but no PRI-23 or PRI-23/30, you will need to use a *crossover cable* to connect the TDM bus to the MVIP connector of the DM card.

To establish the inter-board bus, you'll need a flat bus cable and possibly a crossover cable.

The *flat bus cable* is a 40-pin ribbon cable. The cable can have from 2 to 6 connectors, depending on the adapter configuration of the CyberSWITCH. The ribbon cable connectors are spaced approximately 1 inch apart to mate with the adapter connectors. Never cut a flat cable to shorten it.



Flat Bus (Ribbon) Cable

Some flat cables consist of a primarily grey ribbon, with a single red wire to indicate pin 1. These are essentially the same as the flat bus cable pictured.

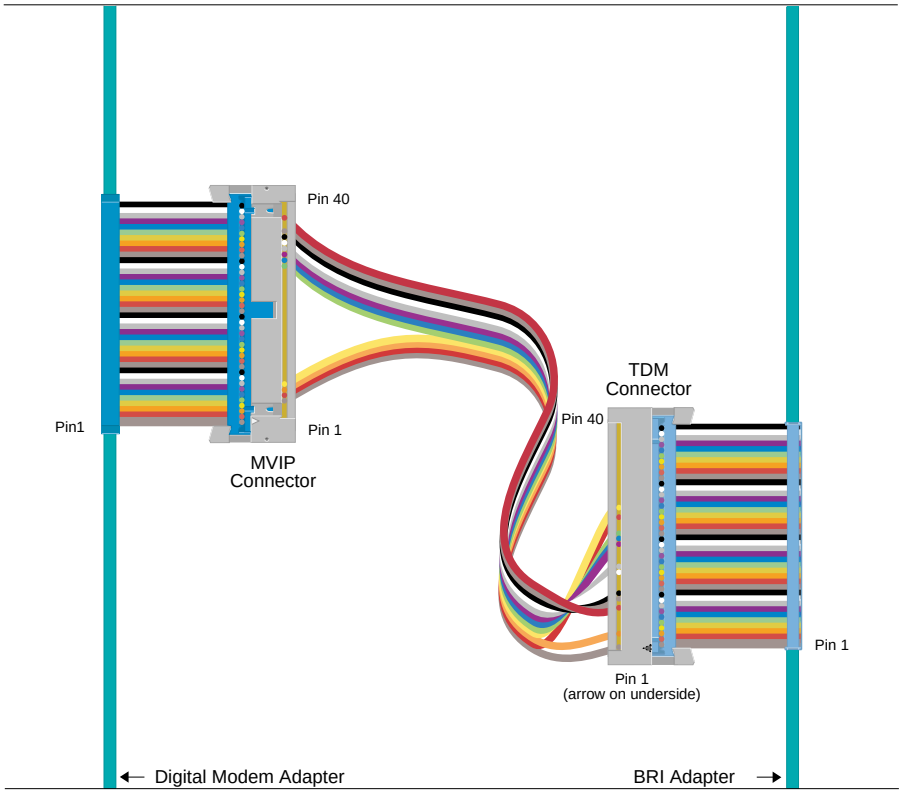
Interconnect all the adapters with the *same connectors* using one flat bus cable of an appropriate length. If your installation combines cards that have TDM-only connectors with cards that have MVIP-only connectors, you will need to use a crossover cable.

The *crossover cable* is a 12-wire ribbon cable with 40-pin connectors. You only need the crossover cable if all the following conditions are true:

- a Digital Modem adapter is present,
- BRI-4, or PRI-8 is present, and
- no PRI-23 or PRI-23/30 is present

Notice that the crossover cable connects between two flat cables. When connecting the crossover cable to the flat cable, align pin 1 on both connectors. Pin 1 is identified by an embossed triangle on the underside of each connector.

The following graphic illustrates a crossover cable application. The adapter with the TDM connector can be one of the following: BRI-4, PRI-8 or Expander.



For crossover cable applications, make absolutely sure that pin 1 (on all six connectors) is aligned so that it is closest to the front panel. Pin 1 is identified by an embossed triangle (or arrow) on the underside of each connector. Note that some cables may be solid grey with one red wire indicating pin 1 (with no identifying triangles).

CONNECTING A WAN ADAPTER TO THE LCD

Note: This cable is only required for systems with an LCD (NE2000-II, 4000, 5000).

The LCD cable is a rainbow-colored cable, approximately 3/4" wide, found inside the system. Locate the embossed triangle on the LCD cable connector. This triangle points to the end of the connector that contains pin 1.

Locate the LCD cable connector on the WAN adapter installed in slot 1. The WAN adapter's LCD cable connector has a "1" labeling the end of the connector that contains pin 1.

Connect the LCD cable to the WAN adapter in slot 1, making sure that the triangle on the LCD cable is at the same end as the WAN adapter's "1" label.

CAUTION:

Failure to line up triangles on LCD cable and WAN adapter's "1" label may result in damage to the LCD.

SUMMARY OF GUIDELINES

CABLING GUIDELINES

Now that you have attached all the inter-board cables, refer to the *connector-type table* and verify that:

1. On BRI-4, PRI-8, PRI-23 and Expander adapters, all TDM bus connectors are connected by a flat bus cable.

2. On PRI-23/30 *only* configurations, all MVIP bus connectors are connected by a flat bus cable. A TDM bus is not used.

3. If mixing PRI-23/30s with BRI-4s or PRI-23s, use both an MVIP bus *and* a TDM bus.

4. When a Digital Modem adapter is installed, it needs to connect to the bus through its MVIP connection.
   - If part of a PRI-23/30 configuration: the DM adapter is part of the MVIP bus.
   - If part of a PRI-23 configuration: you need two buses: one TDM bus for WAN card connections, and one MVIP bus connecting DM adapter with MVIP adapter of the PRI-23.
   - If adapters with only TDM connectors are installed (BRI-4 and PRI-8) and if a DM adapter is installed, then a crossover cable must interconnect the TDM and MVIP buses.

TERMINATION GUIDELINES

On MVIP adapters, the MVIP bus should be terminated on both ends of the bus. Ideally, it should be terminated on the MVIP adapter closest to the CPU (usually the PRI adapter). It should **also** be terminated at the Digital Modem end, on the adapter farthest from the BRI, PRI, or Expander adapter. Termination is enabled by jumpers on DM-8, and switches on the DM-24, DM-24+ or DM-30+, as described earlier. All other MVIP jumpers/switches on all other adapters on the MVIP bus should *not* be terminated.

ACCESSING THE CYBERSWITCH

OVERVIEW

This chapter describes accessing your CyberSWITCH, which includes:

- making proper connections
- establishing an administration session
- accessing Release Notes

MAKING CONNECTIONS

There are a number of ways to make a connection to the system, which include:

- direct connection using a keyboard and monitor
- null-modem connection using a null-modem cable and a PC with Carbon Copy
- remote connection using Telnet
- remote connection using a modem, a remote PC, and one of the following:
  a. Carbon Copy software
  b. PPP Dial-Up Networking software

DIRECT CONNECTION

If you only need to configure or manage the CyberSWITCH in a local environment, the simplest access is through a direct connection. The CyberSWITCH is configured to support a PS/2 or AT-style keyboard and a VGA 15-pin monitor.

Physical Connections:

1. Attach keyboard plug to the keyboard connector located on the back of the CyberSWITCH.
2. Attach monitor cable to the local monitor port located on the back of the CyberSWITCH.

Note: The CSX7000 uses a breakout box for these connections. Refer to the *Local Console Connection* description in the *CSX7000 Guide*. For the location of the keyboard connector and local monitor port for other platforms, refer to the *Hardware Overview* chapter.

Powering On:

1. The rear panel on the system provides an AC input power socket. Plug the standard power cord (supplied with the system) into this power socket.

   CAUTION:
   Some platforms may have a *line voltage select switch* on the rear panel. If you are using such a platform, make sure that this switch is set for the correct AC input power source. When changing the line voltage select switch, make sure the AC power cord is unplugged.

2. Ensure that the POWER-ON button on the CyberSWITCH is in the OFF position.

3. Ensure that the monitor and keyboard are connected to the proper connectors at the rear panel.

4. Plug the power cord into a grounded electrical outlet.

5. Plug the monitor power cord into a proper electrical outlet.

6. Turn on the CyberSWITCH by pressing the POWER-ON button.

7. Turn on the monitor.

8. After a few seconds, power-on initialization will begin. Proceed to *Establishing an Administrative Session*.

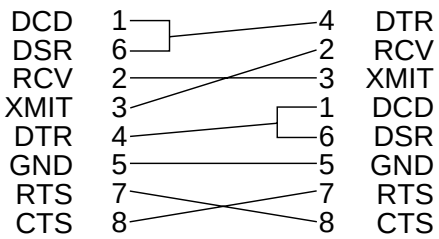
NULL-MODEM CONNECTION TO A PC

If you wish to use an IBM-compatible PC to locally administer your system, you will need to establish a null-modem connection between PC and CyberSWITCH. You will also need the optional Manager diskette which includes Carbon Copy software. Carbon Copy allows you to manage and configure your CyberSWITCH as if it were a direct connection, and additionally provides a means for file transfer. Refer to the *Carbon Copy* discussion in the *Remote Management* chapter for more information.

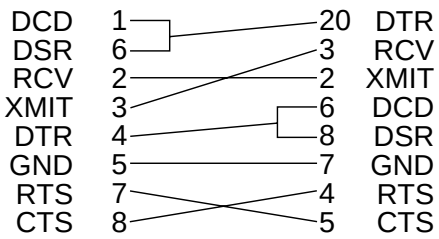
Physical Connections:

1. Use a null-modem cable (with 9-pin female RS232 connectors) to connect the 9-pin, male RS232 port on the CyberSWITCH to the 9-pin, male RS232 port on the PC. Depending on the type of administration console PC you use, the null modem pin-outs may vary. The following are appropriate connections:

CyberSWITCH to IBM AT



CyberSWITCH to IBM PC



2. On the PC, execute the Manager software from diskette, or install the software on your PC's hard disk and execute from hard disk. (1 MB of free space needed for installation.) Note that hard disk operation is more efficient.

Note: You do not need to change Carbon Copy's port parameters. The *default values* are sufficient for null-modem connection.

Powering On:

1. Verify that the *line voltage select switch* is set for the correct AC input power source.

2. Plug the standard power cord into the CyberSWITCH's AC input power socket.

3. Ensure that the POWER-ON button on the CyberSWITCH is in the OFF position.

4. Ensure that the administration console is properly connected to the administration port on the CyberSWITCH.

5. Plug the power cord into a grounded electrical outlet.

6. Power on the CyberSWITCH by pressing the POWER-ON button.

7. Power on the administration console PC. After a few seconds, power-on initialization will begin.

Initiating a Connection:

1. Execute Carbon Copy's *cchelp* program which invokes Carbon Copy for guest operation.

2. Select *Call CC Device* <F1> from displayed menu.

3. Press <ENTER> or <RET>. (No telephone number is necessary since this is a local connection).

4. Carbon Copy will present you with a login prompt. Proceed to *Establishing an Administrative Session*.

REMOTE CONNECTION USING TELNET

Telnet is available by default when IP routing is enabled on the CyberSWITCH.

Note: This type connection is not valid for first-time connections to the CyberSWITCH since you need the CyberSWITCH's IP address for access. However, it is a viable option for routine system management and/or data transfer once initial installation and configuration have been performed.

To access the CyberSWITCH using Telnet, you must have a Telnet client software package. A Telnet client software package is built into the CyberSWITCH. With the CyberSWITCH acting as the Telnet client, simply enter the `telnet <ip address>` command to Telnet into the target host. Refer to the *System Commands* chapter for a complete listing of available Telnet commands.

If you are using a PC as a Telnet client, the PC must have a Telnet client software package. From the Telnet client package, you will access the CyberSWITCH by connecting to the CyberSWITCH's IP address.

LAN access:
To access the CyberSWITCH you must set the device's IP address to be on the same subnet as the CyberSWITCH. Then place the CyberSWITCH on the LAN and Telnet to the address.

WAN access:

1. Connect the system to the (WAN) ISDN line.

2. From a remote device that supports unnumbered IP connections, dial in as a PPP CHAP device USER1 (USER1 as secret). Provide Telnet with the CyberSWITCH address.

3. From a remote device only supporting numbered IP connections, set up an IP Address 2.2.2. 3 and have it dial as a PPP CHAP device USER2 (USER2 as secret). Provide Telnet with the CyberSWITCH address of 2.2.2.2.

After you make a Telnet connection, you will be presented with a login prompt. Proceed to *Establishing an Administrative Session*.

For more information on Telnet, refer to the *Remote Management* chapter.

REMOTE CONNECTIONS (MODEM TO MODEM)

To make modem-to-modem connections, you will need a remote PC and one of the following:

a. *Carbon Copy* software (analog modem to analog modem connection)
b. *PPP Dial--Up Networking* software (analog modem to digital modem connection)

With remote connections using Carbon Copy, you will need a straight-through modem cable, modem and analog connection on the CyberSWITCH side.

With remote connections using Dial-Up Networking software, you will need a digital modem on the CyberSWITCH.

ANALOG MODEM ON THE CYBERSWITCH

Physical Connections:

1. *On the CyberSWITCH side:*
   Connect the 9-pin, male RS232 port on the CyberSWITCH to the modem with appropriate cabling. The CyberSWITCH side of the cable should have a 9-pin female connector. The other end of the cable should have a connector that is appropriate for the modem.

2. *On the remote administration console side:*
   a. Connect the PC to a standard modem.
   b. On the PC, execute the Manager software from diskette, or install the software on your PC's hard disk and execute from hard disk. (1 MB of free space needed for installation). Note that hard disk operation is more efficient. Refer to the *Carbon Copy* discussion in the *Remote Management* chapter for more information.
   c. If necessary, execute *ccinstal* to properly reflect the remote administration port's parameters. Note that Carbon Copy is delivered with the following default settings:

Comm Port Address	COM1
Baud Rate	9600
Modem Type	Direct Connect

Powering On:

1. Ensure that the CyberSWITCH's POWER-ON button is in the OFF position.
2. Ensure that the CyberSWITCH is properly connected to its modem.
3. Plug the CyberSWITCH power cord into a grounded electrical outlet.
4. Power on the CyberSWITCH by pressing the POWER-ON button.
5. Ensure that the remote administration console is properly connected to its modem.
6. Power on the administration console PC.
7. Ensure that Carbon Copy has been installed on the PC and port parameters are correct.

Initiating a Call:

1. Execute Carbon Copy's *cchelp* program which invokes Carbon Copy for guest operation.

2. Select *Call CC Device* <F1> from displayed menu.

3. Supply the telephone number to the modem connected to the CyberSWITCH. Press <ENTER>.

4. Supply password when prompted. The CyberSWITCH recognizes the default password of *CC*. (You may change this password through *ccinstal* if you so choose).

5. Upon successful connection, Carbon Copy will present you with a login prompt. Proceed to *Establishing an Administrative Session*.

DIGITAL MODEM ON THE CYBERSWITCH

Note: This type connection is not valid for first-time connections to the CyberSWITCH since the digital modem is not a preconfigured option. However, it is a viable option for routine system management and/or data transfer once initial installation and configuration have been performed.

Preparing for Connection:

1. *On the CyberSWITCH side:*
   Be sure your Digital Modem adapter and corresponding ISDN lines are properly installed (*Hardware Installation* chapter) and configured (*Configuring Resources and Lines* chapter). You must specify the type of protocol you wish to use: PPP Mode or Terminal Mode. (See *Default Async Protocol* in the *Configuring Advanced Options* chapter.)

   If you wish to use this connection for remote management only, configure the CyberSWITCH for *Terminal Mode*:
   - From CFGEDIT *Options*, select *Default Async Protocol*
   - Select Action on *Data Timeout*
   - Select *Use Terminal Mode*
   - From *Security*, select *Network Login Information*
   - Select *Network Login General Information*
   - Select *Terminal Server Security*
   - Select *Use Administrative Login*

2. *On the remote administration console side:*
   Connect the remote PC to a standard modem. You will need PPP dial-up networking software (such as *WIN95 Dial-Up Networking*) on the PC to initiate your connection to the CyberSWITCH. You will also need the telephone number of the CyberSWITCH.

   If you use *WIN95 Dial-Up Networking* (which supports terminal-type connections), and wish to use this connection for remote management only, be sure to select the option *Bring up terminal window after dialing*.

Initiating a Call:

Follow the specific vendor's instructions for initiating the connection. If you are using this connection for remote management only, proceed to *Establishing an Administrative Session*.

ESTABLISHING AN ADMINISTRATION SESSION

If a login prompt is displayed after the power-on initialization, the system software was preinstalled. Complete the login:

1. The login controls which class of commands the user can access. Each access level (guest or administrator) is protected by a unique login password. This allows managers to assign different responsibility levels to their system users. Enter the following login:
   ```
   admin
   ```

   Note: When using *off-node authentication*, administration access level actually supports up to 101 different login names, from *admin* and *admin00* to *admin99*. These different login names must be configured on the off-node server in order to function properly. For local administration access, only the *guest* and the singular *admin* login access levels are valid.

2. All preinstalled systems are preconfigured with the same password. This is the password that is used the first time a login occurs. Using all lowercase letters, enter the preconfigured password as shown below:
   ```
   admin
   ```

3. It is recommended that the preconfigured password be changed to a user-defined password. To do this, enter the following command at the system prompt:
   ```
   pswd
   ```
   Follow the prompts to change the current password. A password must be a 3 to 16 nonblank character string. Passwords are uppercase and lowercase sensitive.

   Note: User-level security is not available at time of initial installation and configuration. However, once this option is configured, you will have additional security steps before establishing an administrative session. Refer to *Responding to LOGIN Prompts* in the *Configuring Security Level* chapter for more information.

If a DOS prompt is displayed after the power-on initialization, the software has not been preinstalled. You must first boot up with diskette #1 before continuing:

1. Insert software diskette #1 into the system diskette drive.

2. Reboot the CyberSWITCH.

At this point, if you need to install new or upgraded software, refer to the *Upgrading System Software* chapter. If software has been preinstalled by your distributor, skip to *Configuration Tools* chapter to begin the configuration process.

ACCESSING THE RELEASE NOTES

The *Release Notes* provide release highlights and important information related to this release that should be reviewed before you begin the system's installation and configuration. Access these notes via your Web browser: `http://www.cabletron.com/support/relnotes`.

In addition, an abbreviated form of the release notes are in a file called REL_NOTE.TXT. To display the release notes from the CSX system, enter the following command at the system prompt:

[product name]> LIST REL_NOTE.TXT

UPGRADING SYSTEM SOFTWARE

OVERVIEW

This chapter describes how to install system software onto the CyberSWITCH. Instructions are included for the following actions:

- installing system software
- upgrading system software
- accessing Release Notes

The following sections provide instructions to help you complete each of these actions.

INSTALLING SOFTWARE

There is a possibility that your distributor has already completed software installation. Systems with software already installed will prompt the user for a login and a password at the time it is powered on.

If the software has already been installed:
Skip to *Configuration Tools* chapter.

If the software has not already been installed:
Be sure the system was initially booted from diskette #1. Refer to *Establishing an Administration Session* in the *Accessing the CyberSWITCH* chapter.

Continue with this section to complete the software installation. There must be an active administration session before performing the software installation steps.

Note: You should only perform these steps on one system per set of diskettes. Installing these diskettes on more than one system violates your license agreement.

1. Insert the System software diskette #1 (labeled 1 of 4) into the diskette drive.

2. Start the system software installation process by typing the following command at the `A:\` prompt:

   ```
   install
   ```

   An abbreviated version of the Release Notes will be displayed. You will be given a choice of reviewing the Release Notes, or proceeding with the installation. We recommend that you review the Release Notes for release highlights and important information related to this release. See the *Release Notes* section for more information.

   Use <page down> and <page up> to view sections of the Release Notes. At anytime, you may press the <escape> key to continue with the installation.

3. Follow the onscreen instructions to continue with the upgrade. After 2-3 minutes, you will be asked to select the platform type you are installing from a displayed list. Enter the Id of the platform type you are configuring. In most cases, the platform name is on the front of the

machine being installed. If you cannot determine the platform being used, temporarily configure the platform type as "CSX Series," then call Technical Support to help you identify the platform type.

If one of the following messages is displayed:

```
Couldn't open the file C:\SYSTEM\PLATFORM.NEI
Error reading C:\SYSTEM\PLATFORM.NEI
Error reading platform type: there was no "n" in the string
Error reading platform type: type value is too large
Error reading platform type: type was not converted to an int
Error reading platform type: there is no "plat name" field
```

the diskettes you have are corrupted. Call your distributor or Technical Support for a new set of diskettes.

4. The system will copy the files from Disk 1 onto the system disk. Wait for the following message to appear, then remove the system software diskette #1.

```
Remove disk 1 and insert disk 2

Press the enter key when ready to continue installation
```

5. Follow the on-screen installation instructions. The software will provide prompts when you are required to insert the next disk. After installation is complete, the following message will be displayed:

```
System Installation Completed
Release n.n.n
Issue n
```

6. Remove the diskette from the diskette drive and reboot the CyberSWITCH.

7. The log-in screen will now be displayed. It is necessary to enter a log-in and a password. The log-in controls which class of commands the user can access. Each access level (guest or administrator) is protected by a unique log-in password. This allows managers to assign different responsibility levels to their system administrators. Enter the following login:

   admin

   A prompt will appear for an initial password. This user defined password must be a 3 to 16 nonblank character string. Passwords are upper and lowercase sensitive. Enter a password now.

8. The CyberSWITCH program should now be operating.

Note: Before you begin configuring your system, issue the *ver* command to make sure that you have selected the correct platform. If you have not selected the correct platform, reinstall your software and select the correct platform during the installation process.

UPGRADING SYSTEM SOFTWARE

LOCAL UPGRADE

The system upgrade package consists of a set of 3.5" diskettes that contain the necessary upgrade software. These upgrade diskettes may be used on more than one CyberSWITCH.

Once a system is upgraded, you may then upgrade any Manager diskettes purchased for the upgraded system.

Notes: If you have an older platform, there is a possibility that the new features we have added may use up the available memory. Therefore, this release may effect the number of compression sessions available. You may want to purchase more memory for your CyberSWITCH. Contact your distributor.

You may not perform a software upgrade on a system if you will be changing the country version of the software. For example, you may not upgrade a NTT version to a US version; you must instead do an install.

With the availability of the DM-24, modem upgrade is now a possibility. A Digital Modem upgrade is beyond the scope of this section. For more information on upgrading modem firmware, refer to the *modem upgrade* command.

PROCEDURE

1. Insert upgrade diskette #1 into the diskette drive.

2. Issue the *restart* command to restart the platform.

3. At the DOS prompt type the following command to start the upgrade utility:
   ```
   A:\UPGRADE <return>
   ```

   An abbreviated version of the Release Notes will be displayed. You will be given a choice of reviewing the Release Notes, or proceeding with the upgrade. We recommend that you review the Release Notes for release highlights and important information related to this release. See the *Release Notes* section for more information.

   Use <page down> and <page up> to view sections of the Release Notes. At anytime, you may press the <escape> key to continue with the installation.

4. Follow the onscreen instructions to continue with the upgrade. After 2-3 minutes, you will be asked to select the platform type you are installing from a displayed list. Enter the Id of the platform type you are configuring. In most cases, the platform name is on the front of the machine being installed. If you cannot determine the platform being used, temporarily configure the platform type as “CSX Series,” then call Technical Support to help you identify the platform type.

   If one of the following messages is displayed:
   ```
   Couldn’t open the file C:\SYSTEM\PLATFORM.NEI
   Error reading C:\SYSTEM\PLATFORM.NEI
   Error reading platform type: there was no “n” in the string
   Error reading platform type: type value is too large
   ```

```
Error reading platform type: type was not converted to an int
Error reading platform type: there is no "plat name" field
```

The diskettes you have are corrupted. Call your distributor or Technical Support for a new set of diskettes.

5. Follow the on screen prompts for inserting diskettes #2, #3, and #4.

6. If you wish to upgrade the Manager at this time:
   a. issue the *quit* command to terminate the system software
   b. insert the Manager diskette
   c. at the DOS prompt type
      `C:\ADMIN\UG_ADMIN <return>`
   d. follow the on screen prompts to complete the Manager Upgrade

8. Reboot to complete the Upgrade process.

Note: Before you configure your CyberSWITCH, issue the *ver* command and check to make sure that you have selected the correct platform. If you have not selected the correct platform, you must reinstall your software and select the correct platform during the installation process.

HANDLING UPGRADE WARNINGS AND ERRORS

During Step 5 of the Upgrade process, checks are made to ensure that the system is in a "normal" condition before an upgrade. If something abnormal is found, you will be warned of the abnormality and the upgrade process is halted. In the event that you receive any of the following error messages, contact Customer Support for assistance.

Possible errors:

```
Invalid OLD System file.

You can only upgrade from release: n.n.n.
Machine running release: n.n.n.

Could not open old System file.
Cannot run upgrade.
```

REMOTE UPGRADE

The remote upgrade feature will allow you to upgrade the CyberSWITCH by transferring the upgrade file and then remotely issuing a *restart* command. To accomplish this, you will need the `rupgrade.bat` and the latest `autoexec.bat` files, available with 7.2 software.

To remotely upgrade the operational software, follow these steps:

1. From the PC / workstation, Telnet to the CyberSWITCH and login as admin.

2. Verify that the system is ready to receive TFTP upgrades:
   - Enter MANAGE MODE by typing *manage* <RET> at the system prompt.
   - Using the MANAGE MODE command *tftp*, verify that:

    - TFTP feature is enabled
    - TFTP server is enabled
    - TFTP server is assigned ADMIN file access rights
  - Using the MANAGE MODE command *fileattr*, verify that:
    - ADMIN has READ/WRITE access to CONFIG files
    - ADMIN has READ/WRITE access to OTHER files
  - Exit MANAGE MODE by typing *exit* <RET>.

3. *If you are upgrading to Release 7.2 software,* perform the following:
   - Using the TFTP client on the remote workstation, TFTP PKUNZIP.EXE to the `\admin` directory of the CyberSWITCH to be upgraded.
   - TFTP RUGRADE.BAT to the \ (root) directory.
   - TFTP AUTOEXEC.BAT to the \ (root) directory.

   If you are upgrading from Release 7.2 to a later release, skip this step. (These files are already included in 7.2 software).

4. Using the TFTP client on the remote workstation, TFTP UPGRADE.OSW to the \ (root) directory of the CyberSWITCH to be upgraded.

   Notes: If you experience a transmission timeout, check the retransmission setting on the TFTP package. A retransmission rate of 10 seconds is usually sufficient; values less than that may not work properly.

   If you experience a problem transferring the file with TFTP, wait about three minutes for the TFTP to fail, delete the incomplete file, and try again.

5. Telnet to the CyberSWITCH and issue the *restart* command.

ACCESSING THE RELEASE NOTES

The *Release Notes* provide release highlights and important information related to this release that should be reviewed before you begin the system's installation and configuration.

An abbreviated version of the Release Notes are in a file called REL_NOTE.TXT. This file will automatically display upon initial install or upgrade. If you wish to view these notes at another time, enter the following command at the system prompt once the system is up and running:

[product name]> LIST REL_NOTE.TXT

You may also access the complete set of Release Notes via your Internet Web browser:

`http://www.cabletron.com/support/relnotes`

BASIC CONFIGURATION

We define basic configuration as the configuration needed by most users. Basic configuration will get your system up and running. Note that not all configuration steps in this part are required. For example, if you are only using bridging, you will have no need to complete the configuration steps included in Configuring Basic IP Routing.

We include the following chapters in the *Basic Configuration* segment of the *User's Guide*:

- *Configuration Tools*
  A description of the configuration tools provided for configuring the CyberSWITCH.

- *Configuring Lines and Resources*
  Instructions for configuring your system's lines and resources.

- *Configuring Basic Bridging*
  Instructions for configuring your system's basic bridging information. Basic bridging includes enabling / disabling bridging and bridge dial-out.

- *Configuring Basic IP Routing*
  Instructions for configuring your system's basic IP routing information. Basic IP routing includes enabling / disabling IP, IP operating mode, network interfaces, static routes, and enabling / disabling IP RIP.

CONFIGURATION TOOLS

OVERVIEW

We provide the following configuration tools to set up and / or alter your configuration:

- CFGEDIT, the configuration utility
- Manage Mode, the dynamic management utility

CFGEDIT is the comprehensive utility you use to initially set up your system; you may use it later to make configuration changes as well. However, CFGEDIT is NOT dynamic. This means you will have to interrupt normal system operations in order to update configuration files. (You may do so by either rebooting, or issuing the `restart` command).

Manage Mode provides a real-time management mechanism that allows you to change the configuration, without interrupting the current execution state of the system software. But, because it is dynamic, Manage Mode does have its limitations. So, when making configuration changes, you usually need to use a combination of both of these two tools.

You may only have one CFGEDIT or Dynamic Management session active at a time per system. For example, if a user is making changes directly to the system using Dynamic Management, and then a second person at a different location using Telnet attempts changes, access will be denied to the second person.

With two exceptions, it is possible to completely configure your system using CFGEDIT. The exceptions are:

1. TFTP configuration
2. file attributes configuration

These two elements can only be configured using Manage Mode.

CFGEDIT

CFGEDIT is a menu-driven utility. It consists of multiple, detailed submenus which allow you to set up or change configuration parameters. To better understand the structure of CFGEDIT, refer to the *CFGEDIT Map*.

CFGEDIT allows you to configure your system while the system software is still executing. These configuration changes are saved in a temporary copy of configuration data. At a convenient time, you may then reboot the system to make these changes permanent.

EXECUTING CFGEDIT

After the system software has been loaded, you can start CFGEDIT by entering the following command at the system prompt as shown below:

```
[product name]> cfgedit
```

As long as there is no other "change" session active (CFGEDIT or Manage Mode), access is granted, and the following menu is displayed:

```
 Main Menu:

   1) Physical Resources
   2) Options
   3) Security
   4) Save Changes

Select function from above or <RET> to exit:
```

From this screen you will begin the configuration process. Refer to *Basic Configuration* and succeeding chapters for details on using this utility to perform specific configuration tasks.

Remember, changes to CFGEDIT are NOT dynamic. Changes are saved in a temporary copy of configuration data, and will not affect the current operation of the system in any way.

SAVING CFGEDIT CHANGES

To terminate the session, return to the main CFGEDIT menu. If you have made changes, select option 4 (*Save Changes)* before exiting. If you attempt to exit without saving, you will be prompted to do one of the following:

- save changes (Y) and exit
- do not save changes (N) and exit
- do not save changes as yet, but return to the Main Menu for further configuration <RET>

To save changes at this point, answer Y for yes:

```
Save changes and exit (Y or N)? or press <RET> for previous menu:
```

The save process also includes all unsaved Manage Mode changes which were made prior to the CFGEDIT session, if any.

At your earliest possible convenience, restart the CyberSWITCH. This will then activate the new configuration data.

DYNAMIC MANAGEMENT

EXECUTING DYNAMIC MANAGEMENT

The Dynamic Management feature provides a real-time management mechanism; allowing you to change the system's configuration without interrupting the execution of the system software. This feature consists of console commands that enable you to display current system parameter, change many parameters dynamically, and write changes to disk files so that they remain permanent.

Before using Dynamic Management commands, you must first enter the special Manage Mode by typing the following command at the system prompt:

```
>manage
```

Once Manage Mode is entered, the prompt changes from [system name]> to [system name]: MANAGE>. While operating in Manage Mode, only Dynamic Management commands are available. All other system commands are ignored until you exit Manage Mode.

The <CTRL><C> key sequence will terminate the current command and return you to the MANAGE> prompt. This is useful if you are in the process of responding to a series of prompts and you wish to abort the command without responding to the remaining prompts.

Note: To use a command, you may enter the full command name as it appears in the HELP list, or you may shorten the command to the point that it can still be distinguished from all other Dynamic Management commands.

UTILITY DYNAMIC MANAGEMENT COMMANDS

There are several Manage Mode commands that are used for functions other than to configure the system. They are as follows:

cls
Clears the display screen. This command is also available as an administration command.

help
The Manage Mode help command lists the available Dynamic Management commands and instructs the user to enter the command followed by a question mark to see help information for that specific command.

readme
Displays helpful tips on how to use the Dynamic Management commands.

SAVING DYNAMIC MANAGEMENT CHANGES

The Dynamic Management commands allow system data to be changed in real-time. These changes take effect immediately upon the execution of the command and remain in effect until the system is restarted. Once a software restart occurs, the changes are lost because the software reads its initial system data values from a series of configuration files.

To prevent desired data changes from being overwritten by the restart process, the *commit* command should be executed. This command writes the current system data to the appropriate disk files, thus making all changes permanent, even if the system software is restarted.

The *commit status* command displays the number of dynamic changes that have been made using each Dynamic Management command since the last *commit* was performed.

To return to the normal operating mode after you have committed your changes, issue the following command:

```
MANAGE> exit
```

USING THE NETWORK WORKSHEETS

Please take the time to fill out the requirements worksheets located in *System Worksheets*. The requirements worksheets are:

- Network Topology Worksheet
- System Details Worksheet
- System Device List Worksheet(s)
- Bridging / Routing Worksheets

These worksheets will be helpful in configuring and managing your system. They capture important network information. To see examples of completed worksheets, refer to the *Example Networks Guide.*

USING THE CONFIGURATION CHAPTERS

The configuration chapters follow a basic format for explaining the configuration process of each system feature. The format is:

1. A brief outline of the configuration procedure using CFGEDIT (if applicable).

   Note: In this guide we have included a *map* of the configuration utility CFGEDIT.

2. A brief outline of the configuration procedure using Manage Mode (if applicable).

3. A definition of each configuration element.

4. Background feature information providing a more detailed explanation of the feature.

CONFIGURING RESOURCES AND LINES

OVERVIEW

This chapter describes the configuration of physical resources, lines and subaddresses.

Resources refer to the hardware adapters that plug into the CyberSWITCH. For example, a WAN resource is the physical component (i.e., interface) for the attachment of lines (or connections) to your system.

Lines are communication facilities from the carriers. These lines directly attach to your system. From the system perspective, lines provide the physical connection to switched networks. Lines are not required for LAN connections.

There is an optional element, the system *subaddress*, that you may configure for a point-multipoint line. This element is a call screening method. A subaddress is only needed if you have a line interface type of point-multipoint, and you choose the subaddress call screening method.

RESOURCES

CONFIGURING RESOURCES

USING CFGEDIT

To configure the CyberSWITCH's resources, select *Physical Resources* from the Main Menu. The following will then be displayed:

```
Physical Resources

   1) Resources
   2) Data Lines
   3) Accesses
   4) ISDN Subaddress

Select function from above or <RET> for previous menu:
```

1. Press 1 to begin the configuration of the resources.

   Notes: Unconfigured resources will cause your system to operate in an unpredictable manner. Using the following instructions, configure only those resources you plan to use.

   The COMMPORT resource is a preconfigured resource. You cannot delete this resource.

2. Select *Add* to add a resource. Select the resource type.

   Notes: Do not select the BASIC_RATE_NET resource type. This is used for demonstration purposes where BRI lines are not available.

3. Enter the resource's slot number. Refer to the packing slip or the back of your system for the correct slot number for each resource.

4. For BRI and PRI resource types: select the proper BRI / PRI switch type for the lines you will be using. The *table* in the *Overview* identifies which switch types are available; your carrier will identify which particular switch is used in your area. If you select the NET3 or NET5 international switch, you will be prompted for the region of operation:

```
1)              DEFAULT
2)              AFRICA
3)              AMERICAS
4)              ASIA
5)              EUROPEAN
6)              PACIFIC-RIM

Region from above [default = 1]:
```

   Select the appropriate region. Based upon the region you select, you will be presented with a list of countries. Select the country of operation from this list. If you cannot find your country on any list, return to the Region Menu and select the default value (1).

   For PRI resource types only:
   a. Select the correct synchronization type. Select either clock master or clock slave. If unsure, configure as "Slave."
   b. For a PRI_4ESS carrier switch type, select which software load (generic #) the switch is running. Obtain this information from your carrier.
   c. For a Teleos Simulator carrier switch type, select the switch type that Teleos is simulating.

5. For the Digital Modem resource type:
   a. Select from DM-8, DM-24, and DM-30. Note that DM-24 refers to both the V34+ modem adapter as well as the K56Flex modem adapter. If you specify DM-24, the CyberSWITCH will distinguish between the two.
   b. Select the Pulse Code Modulation (PCM) encoding method appropriate for your country. Choices include mu-law and A-law.

6. For encryption resource types:
   From the list of resource types, choose *DES_RSA*. (Refer to the *Configuring Encryption* chapter.)

USING MANAGE MODE COMMANDS

resource
Displays the current resource configuration.

RESOURCE CONFIGURATION ELEMENTS

RESOURCE TYPE
The type of adapter (resource) that plug into the system. WAN adapters are the physical interface for the attachment of lines (i.e., connections) to your system.

RESOURCE SLOT
The slot number into which the resource is plugged.

SWITCH TYPE
For ISDN resources (BRI and PRI) only. The switch type you wish to configure.

REGION
For NET3 and NET5 switchtypes. When configuring switches, first identify the region of operation, and then the country.

COUNTRY
For the NET3 and NET5 switchtypes. The country in which the system is operating.

GENERIC NUMBER
For PRI_4ESS primary rate switch type only. The software load (generic #) the switch is running.

SYNCHRONIZATION TYPE
For Primary adapters only. Every framed transmission line requires a clock source from which it must derive the appropriate bit timing and channel timing relative to the start of a frame. For most CPE gear, the clocking is derived from the received signal and the transmission clock is thus a "slave" to the network. However, if the line is to provide its own clocking, it must derive a clock from an internal source rather than a received signal. The line is then a "master" clock source.

PCM ENCODING METHOD
For DM-24 and DM-30 adapters only. Pulse Code Modulation (PCM) is a common method of encoding an analog signal into a digital bit stream. PCM encoding choices are:
- mu-law (the PCM encoding standard used in Japan and North America)
- A-law (the PCM encoding standard used in Europe)

RESOURCE BACKGROUND INFORMATION

The basic rate (BRI) resource directly terminates a standard USOC RJ45 connector. It is supplied with a standard S/T interface. A U interface option is not available for this adapter. The BRI resource supports 1 or 4 connections/ports depending on which option you purchase. It provides support for the following switch types:
- NTT
- 5ESS
- DMS100
- NI1
- 1TR6
- NET3
- Definity
- Legend
- TS0-13

BASIC RATE NET is a test facility. This should not be configured as a resource type.

The T1-E1-PRI can be used for any T1, E1, or PRI resource, and directly terminates a standard USOC RJ45 connector. It is supplied with a standard S/T interface and supports one port. It also provides support for the following switch types:
- NTT
- 4ESS
- 5ESS
- Definity
- DMS100, DMS250, DMS500
- SL100
- NET5

- 1TR6
- TS0-14

The expander resource provides additional connections to the PRI resource. It supports eight additional connections.

The V.35 resource provides two standard V.35 connections when used with the V.35 adapter cable.

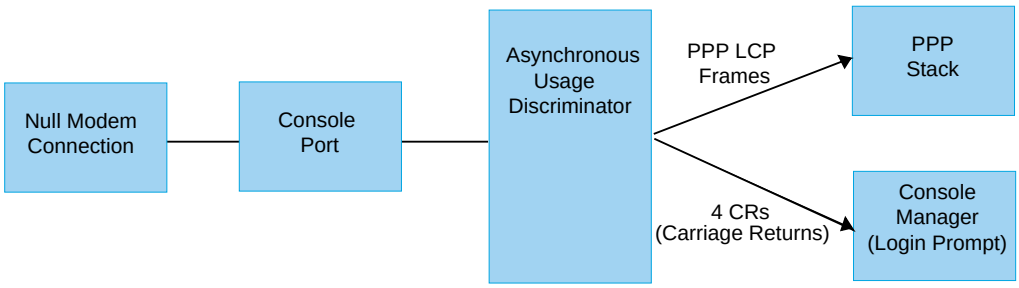
The RS232 resource provides four standard RS232 connections when used with the RS232 adapter cable.

The ethernet-2 resource provides direct support for two standard AUI LAN connections. The ethernet-1 resource provides direct support for one standard AUI LAN connection. These AUI interfaces provide connections for 10Base2, 10Base5 or 10BaseT transceivers.

The COMMPORT resource provides access to the CyberSWITCH's serial port (COM 1) for serial (asynchronous) communications. This includes access for local console management, as well as local async-PPP data transfer.

The following figure illustrates how the CyberSWITCH handles this asynchronous data when it is in autosense mode (the system default). The data arrives through the COM 1 port, and is sent to an internal Asynchronous Usage Discriminator (AUD), which monitors the data stream. The AUD determines if this is to be a PPP connection, or a remote console connection. This determination is made within a configurable time frame:

- if the *AUD detects PPP LCP frames*, it connects the data to a PPP stack. The CyberSWITCH sends the data to the LAN as appropriate.
- if the *AUD detects four carriage returns* from a console device, it will provide analog console access by presenting a CyberSWITCH login prompt to the console.
- if neither situation is detected within the configured time frame, the connection is turned over to PPP.



The DM-8, DM-24, and DM-30 are digital modem resources. The *numbered suffix* identifies the number of modems on the particular resource (i.e., DM-8 has 8, DM-24 has 24, etc.). These resources are used with BRI, PRI, or Expander resources to provide connectivity to remote devices by modem. More than one DM resource may be used to provide modem connections; however, the number of connections is limited by the number of available ISDN channels, ISA / EISA card slots, and ISA / EISA interrupts. There is a four card maximum for the number of DM-8s per system, and

a three card maximum for DM-24s or DM-30s. These cards may also be combined (for example, a DM-8 along with two DM-24s), as long as you adhere to the lower card maximum per system.

LINES

CONFIGURING LINES

Note: There is a preconfigured serial line named *ASYNDMPORT* to parallel the preconfigured serial resource (COMMPORT). You may not delete this line; however, you may change the line's values (including the default mode of operation).

USING CFGEDIT

To configure lines, select *Data Lines* from the *Physical Resources* menu. Follow instructions for the type of line you are configuring:

CONFIGURING A LINE FOR A BRI RESOURCE

1. Enter the line name.

2. Select the line's slot and port combination.

3. Choose either a point-to-point or a point-multipoint interface type.

4. If you select a line interface type of point-multipoint, you will need to choose one of the following call screening methods: none, subaddress, or telephone number. If you choose the subaddress screening method, you must configure a subaddress. Refer to *Configuring a Subaddress*.

5. Add the necessary data links.
   a. Select Automatic TEI Negotiation UNLESS this is a point-to-point NTT line.
   b. If you need to assign a TEI Negotiation value, the default value of 0 is normally correct.
   c. Only if you plan on using X.25 over the D-Channel on this line, answer *yes* to the following prompt:

```
Will this Data Link support X.25 communications (Y/N)? [default N]
```

6. If the line uses a NI-1 or a DMS-100 switch type, you must also enter the following:
   a. SPID(s) - supplied by your carrier
   b. Directory Number(s) associated with the SPID(s) - supplied by your carrier
   c. Number of digits to verify.

CONFIGURING A LINE FOR A PRI RESOURCE

1. Enter the line name.

2. Select the line's slot and port combination.

3. Select following line characteristics:
   - framing type
   - line coding type
   - T1 signaling method

   If you are unsure of your line's characteristics, try the following defaults:

Characteristic	*PRI/T1 lines*	*E1 line*
Framing type	ESF	Multiframe CRC
Line coding type	B8ZS	N/A
Signaling Method	Common_Channel	N/A

4. Select the correct T1 line build out value (US only). If you are using an external CSU, specify a short haul build out (line length in meters). If you do not have an external CSU, specify a long haul build out (decibel attenuation value from Telco).

5. A data link is assigned to the line upon completion of the line configuration. Add more data links or modify the existing data link.
   a. Only if you plan on using X.25 over the D-Channel on this line, answer *yes* to the following prompt:

```
Will this Data Link support X.25 communications (Y/N)? [default N]
```

   b. Assign a TEI Negotiation value of 0.

Note: If you select E1/R2 signaling for your framing type, you will not be asked to configure datalinks (items 4 and 5). R2 signaling does not make use of a datalink; all datalinks associated with the line are automatically deleted.

If you select a Robbed Bit line, CFGEDIT will inform you that RBS will delete any datalinks on the line. The system will prompt you to confirm this deletion, and then automatically delete the datalinks.

CONFIGURING A LINE FOR V.35 AND RS232 RESOURCES

1. Enter the line name.

2. Select the line's slot and port combination.

3. Select the line type.

   Note: The network line type is designated for lines used by a Dedicated Access, Frame Relay Access, or X.25 Access.

4. Select the data line idle character. The default value is *marks.* However, there may be some receiving devices which cannot properly make this determination with the default of idle marks. If communication cannot be established with the receiving device, you may need to take

care that the idle character is set to a value that the receiving device will understand. For example, CISCO devices require the flag data line idle character.

CONFIGURING CHANGES FOR A COMMPORT RESOURCE

1. Select *Change* from the *Data Lines* menu of *Physical Resources.*
2. Select ASYNCDMPORT.
3. You will be prompted to accept the default or provide new information for the following:
   a. baud rate
   b. data bits
   c. stop bits
   d. parity value
   e. flow control type
   f. mode:
      - Autosense (default): can be either terminal or PPP-async. Requires user interaction (four carriage returns) to get to terminal mode.
      - Term: terminal mode only. Login prompt automatically sent to remote console.

USING MANAGE MODE COMMANDS

line

Displays the current line configuration.

datalink

Display the current data link configuration.

datalink add

Allows you to add a data link. The following sample screen shows how a data link is added.

```
Current LINE Configuration:

id     LINE NAME             TYPE                SLOT       PORT
-------------------------------------------------------------------------------
1      LINE.BASICRATE1       BR_ISDN              1         1
2      LINE.BASICRATE2       BR_ISDN              1         2
3      DMS100.LINE1          BR_ISDN              2         1

Select line id for new data link or press <RET> to cancel: 3<RET>

Automatic TEI negotiation (Y or N) [default = Y]? N<RET>

TEI value [default = 1]? <RET>

Service Profile ID (enter 0 for no SPID)
[default = NO SPID]? 13135551212<RET>

Directory number [default = 13135551212]? 5551212<RET>

Number of digits to verify [default = 7]? <RET>

The DATALINK configuration has been updated successfully.
```

datalink change

Changes an existing data link.

datalink delete
Deletes an existing data link.

LINE CONFIGURATION ELEMENTS

LINE NAME
A 1 to 16 user-defined character string (using all non-blank characters) that identifies the line. Each line must have a unique name.

LINE SLOT
The slot number assigned to the resource that will terminate this line.

LINE PORT
The port number of the resource that will terminate this line.

LINE INTERFACE TYPE
For basic rate lines only. Choice of point-to-point or point-multipoint. The point-to-point interface type is the type most often used in the U.S.; point-multipoint is most often used in Japan.

AUTO TEI
For basic rate lines only.The default setting for automatic TEI negotiation is "yes". For #5ESS and DMS100 lines, you should not change the setting. For NTT point-to-point lines, you should disable the automatic TEI negotiation by answering "no" to the prompt for this feature.

CALL SCREENING METHODS
For basic rate lines only. If you select a line interface type of point-multipoint, choose one of the following call screening methods: none, subaddress, or telephone number. The paragraphs below define each method.

1. None
   All calls will be accepted.

2. Subaddress
   Uses a configured subaddress for this site. If the subaddress method is chosen, and a subaddress has not been configured for this site, an error message will be displayed. You must either choose another method, or configure a subaddress for this site.

3. Telephone Number
   Telephone number(s) for your site used for call screening. Only calls directed to that specific telephone number will be accepted. If there is more than one, enter the list of telephone numbers separated by commas. After entering the telephone numbers, you will then be asked to enter the maximum number of digits (starting at the rightmost digit) to be verified.

   Note: If the telephone number(s) entered here do not exactly match the number(s) for the site, you will be warned at this time. (The number of digits compared will be the number of digits you chose to use for verification.)

DATA LINKS
A data link is a data communications link to the telephone switch. Your Carrier Service can provide you with the data link values you need to configure. All switch types, except the DMS100 and the NI-1, require a single data link per line. The NI-1 switch type can have either one or two data links per line. The DMS100s generally require two data links per line, one for each B channel. For both

NI-1 and DMS100 switch types, contact your Service Provider for the number of data links required.

The table below summarizes the number of data links and SPIDs that are required for each switch type.

Switch Type	*Number of Data Links*	*Number of SPIDs*	*Number of Directory Numbers*
DMS100 custom	2	2	2
NI-1	1 or 2	1 or 2	1 or 2
all other	1	0	0

When adding a data link for BRI lines, designate whether to use Automatic TEI Negotiation. Automatic TEI Negotiation is used UNLESS this is a point-to-point NTT line. If you do not use Automatic TEI Negotiation, a TEI value is required. The default TEI value is 0, which is normally correct for a point-to-point NTT line. For PRI lines, use the default TEI value of 0.

Data links are handled differently for DMS and NI-1 switches. For most switches, the BRI line has only one phone number (for the Data Link), but it can handle two calls (one for each bearer channel). For DMS and NI-1 switches, the BRI line has two SPIDs, and two phone numbers. Note that either SPID can use either bearer channel. There is no one-to-one correspondence. You must enter the number of digits to verify (starting at the right-most digit), so that when the system receives a phone call it can determine on which bearer to accept the phone call. The maximum number of digits should be 7, which is the default value in most cases.

SERVICE PROFILE ID (SPID)
For basic rate lines only. SPIDs are only required for DMS100 and NI-1 switch types. A SPID is a number that identifies ISDN equipment attached to your ISDN line. Depending on the type of ISDN service you have, you may have one, 2, or no SPIDs. When ordering your ISDN service, your service provider should supply you with SPID information.

A SPID is usually derived from the ISDN line's telephone number. It may include the area code. It may also include a special prefix and / or suffix (for example, a prefix of 9 for Centrex lines).

The SPID format for AT&T 5ESS NI-1 Service is:

01nnnnnnn0tt

where nnnnnnn is the 7 digit phone number (no area code) of the BRI line
tt is a user assigned 2 digit terminal Id code, 00 is normally used

The SPID format for AT&T 5ESS Custom Multipoint Service is:

01nnnnnnn0

where nnnnnnn is the 7 digit phone number (no area code) of the BRI line

The SPID format for Northern Telecom DMS-100 NI-1 Service is:

aaannnnnnnss

where aaa is the 3 digit area code of the BRI line
nnnnnnn is the 7 digit phone number of the BRI line
ss is the SPID suffix (optional, 01 can be used for one number, 02 for the other)

The SPID format for Northern Telecom DMS-100 Custom Service is:

aaannnnnnnsstt

where aaa is the 3 digit area code of the BRI line
nnnnnnn is the 7 digit phone number of the BRI line
ss is the SPID suffix (optional, 01 can be used for one number, 02 for the other)
tt is a user assigned 2 digit terminal Id code, 00 is normally used

If the DMS100 requires two data links per line, it will also have two "Service Profile Identifiers (SPIDs)" and two directory numbers. If the NI-1 has two data links per line, two SPIDs and two directory numbers are required, otherwise one SPID and one directory number is required. A SPID is paired with a directory number to define a data link.

Note that if your line does not require a SPID, enter a SPID value of 0.

DIRECTORY NUMBERS

If your line requires a SPID (if you entered a SPID with a value other than "0"), you will be required to enter the site's directory number. That directory number is paired with the above entered SPID for this data link. The directory number is used to match an incoming call with the correct data link.

DIGITS VERIFIED

The number of digits to verify (starting at the rightmost digit), so that when the system receives a phone call it can determine on which bearer to accept the phone call. The maximum number of digits should be 7, which is the default value in most cases.

FRAMING TYPES

For primary rate lines only. The normal line transmission method employed on a PRI line is a time-division multiplexed (TDM) scheme of repeating fixed-length frames.

For T1 lines, each frame uses a single bit to convey such things as a frame alignment pattern, data checksums, and in more advanced networks, maintenance commands between the network and the Customer Premise Equipment (CPE). For E1 lines, all of channel 0 is used for this. The two most common framing types for PRI/T1 lines are SF and ESF, which are 12- and 24-frame formats, respectively.

E1 lines can use one of the following framing types:

- doubleframe
- multiframe with no CRC
- multiframe with CRC
- R2 signaling

  The *R2 signaling* method uses one channel of the PRI frame to do line signaling, and then uses in-band tone pairs to complete the call control messaging. This type of signaling is common in Korea and other non-North American countries. R2 signaling is only available in systems with Digital Modem resources.

LINE ENCODING

For Primary Rate lines only. Line encoding specifies the nature of the signals that are used to represent binary one and zero at the physical layer. Two encoding methods are Alternate Mark Inversion (AMI) and Bipolar 8 Zero Substitution (B8ZS). AMI as the encoding scheme implies that the applications using the transmission line must guarantee a certain number of 1s in the signal to help prevent a loss of synchronization in the network. This is possible if the voltage level of the signal remains zero for too long a period of time (i.e., too many logical 0s in the transmitted data). B8ZS enforces no such limits on the application using the transmission medium since it introduces bipolar violations in the signal. These violations are in turn interpreted at the receiving end not as errors, but simply as the substitution of a 1 for a 0 after certain number of consecutive 0s were detected in the transmitted signal.

T1 SIGNALING METHOD

For primary rate lines only. The signaling method dictates how and where the call signaling is to be carried. The methods currently available are: Common Channel and Robbed Bit Signaling.

COMMON CHANNEL

In the Common Channel signaling case, one of the 24 channels of the PRI frame is devoted to call control messaging.

ROBBED BIT SIGNALING

In the Robbed Bit Signaling method, 1 bit of each data channel is "robbed" in order to carry the requisite signaling information. This method is only available for Digital Modem resources.

Notes: Mixing RBS lines and Common Channel lines in a single CyberSWITCH will cause some problems with outbound calls. A 64 Kbps data call may try to go out on the RBS line. The WAN card controlling that line will reject the call, as will every other WAN card until a card using a Common Channel line is tried.

The E1/R2 signaling method is specified under Line Characteristics, *Framing Type*.

LINE BUILD OUT

For primary rate lines only. No matter what the quality of the cabling employed in a network, each and every line experiences some signal loss or degradation. Line Build Out describes the degree of attenuation to be applied to the transmission signal in order to have the correct signal levels and shape arrive at the receiver. Generally, the longer the line connecting the CPE and the network equipment, the less the transmitted signal is attenuated.

CFGEDIT will use short or long haul information to determine the correct Line Build Out (i.e., degree of attenuation) for your lines. The value you input (in CFGEDIT) to determine attenuation depends on whether or not you are using an external Channel Service Unit (CSU).

If you are using an external CSU, you will specify a value under *Short Haul Build Out*. Specify the length of the line, in meters, from CPE to the CSU by selecting a range from zero to 210 meters.

If you are not using an external CSU, specify a value under *Long Haul Build Out*. On long hauls, your telephone company will provide you with a decibel attenuation value when they install the lines. The installers may specify option labels *A*, *B*, or *C* during installation. If so, these labels correspond, respectively, to Long Haul Build Out values of *-0.0dB*, *-7.5dB*, and *-15.0dB*. The value is dependent on distance, type and condition of physical line, and other environmental factors. For example, if the distance to the Telco switch is great (6000 foot maximum), or the line is old, you may need a

decibel value of 0.0 (meaning no attenuation). If the distance is much closer (for example, 1000 ft.), the decibel value may be -15.0 (i.e., the signal is strong enough that it needs a certain amount of attenuation).

LINE TYPE
For V.35 and RS232 lines only. This parameter differentiates the network connections from connections to local computing devices. The network line type should be specified for lines that will be used by a Dedicated, Frame Relay, or X.25 Access.

DATA LINE IDLE CHARACTER
This identifies the idle character which is transmitted by the CyberSWITCH between the HDLC frames. The character choices are marks (all '1's) or HDLC flags (hexadecimal '7E'), with marks being the default. In most situations, the default value is acceptable, as the receiving side should able to identify the start of a new frame after reception of either idle character. However, there may be some receiving devices which cannot properly make this determination with the default of idle marks. If communication cannot be established with the receiving device, you may need to take care that the idle character is set to a value that the receiving device will understand. For example, CISCO devices require the flag data line idle character.

COMMPORT INFORMATION
For systems using the asynchronous management port (COMMPORT) for out-of-band management. These elements control how the port will function. Elements include:

- modem name
- baud rate
- data bits
- stop bits
- parity value
- flow control type
- mode of operation

Mode of operation determines whether this port operates in autosense mode or terminal mode. *Autosense mode* offers the flexibility to use this port for console access, or to send PPP-async data. For console access, the remote user must press <Enter> or <Return> four times upon call connection. If no carriage returns are detected, the CyberSWITCH assumes it will receive PPP data.

Terminal mode requires no interaction. It automatically sends the attached device a login prompt for console access.

LINE BACKGROUND INFORMATION

Lines are communication facilities from the carriers. These lines directly attach to the system. From the system perspective, lines provide the physical connection to switched networks. Lines are not required for LAN connections.

Lines must be configured for BRI resources and PRI resources. For PRI resources, the CyberSWITCH supports both T1 lines (used in North America, Australia and Japan) and E1 lines (used in Europe, Mexico, South America, Korea). To specify the type of line as either T1 or E1, you need to set a hardware switch on the PRI resource itself. (See *PRI adapter settings* in the *Hardware Installation* chapter.)

When configuring PRI lines, you will need to specify framing type, line coding type, and T1 signaling method. Refer to the *Configuration Elements* section, which describes these characteristics.

R2 SIGNALING

R2 Signaling is a particular framing type commonly found in Korea and other locations outside of North America. With 7.3 software, this feature will be available for Korean markets only. This feature allows the CyberSWITCH to accept incoming calls and create outgoing calls over E1 lines provisioned for R2 signaling. The CyberSWITCH treats the R2 user or device just as it would a digital modem user.

To use R2 signaling, you must enable the R2 signaling option for an E1 PRI data line in CFGEDIT. You may configure individual channels on the line for dedicated access or frame relay access, provided that the sixteenth time slot of the frame remains available for line signaling, and the line signaling bits associated with the access remain idle.

Prerequisites for using R2 signaling:

- Use with a PRI-23/30 resource only. This resource has the proper hardware support to enable the signaling stack. Refer to the *PRI-23/30* switch settings.
- Use with a DM-24+ or DM-30+digital modem resource. (The system relies on digital modems for signaling and connecting incoming calls).
- Configure R2 users or devices for digital modem access. The dialout phone number for an R2 user will be under the digital modem configuration.
- Do not mix R2 and normal ISDN traffic on the same E1 interface.
- If mixing R2 and ISDN resources within the same CyberSWITCH, be sure to use the Bandwidth Reservation feature in order to insure that outgoing calls are made over the proper lines.
- When using E1/R2 signaling, the CyberSWITCH supports a maximum of 3 PRI resources and 3 digital modem resources per system.
- There is a one signaling session per incoming channel.

SUBADDRESSES

CONFIGURING A SUBADDRESS

USING CFGEDIT

1. To configure a subaddress, select *ISDN Subaddress* from the *Physical Resources* menu.

2. Enter the subaddress. The subaddress is supplied by your Carrier Service.

SUBADDRESS CONFIGURATION ELEMENTS

SUBADDRESS
The subaddress for the system.

SUBADDRESSES BACKGROUND INFORMATION

A subaddress may be configured for a point-multipoint line. This element is a call screening method. A subaddress is only needed if you have a line interface type of point-multipoint, and you choose the subaddress call screening method.

CONFIGURING BASIC BRIDGING

OVERVIEW

This chapter provides information for configuring basic bridging features. Basic bridging configuration includes:

- enabling / disabling bridging

A separate chapter, *Configuring Advanced Bridging*, provides information for configuring advanced bridging features. Advanced bridging features include:

- bridge dial out
- Spanning Tree Protocol
- mode of operation
- bridging filters
- known connect lists

MAC LAYER BRIDGING OPTION

ENABLING/DISABLING BRIDGING

USING CFGEDIT

1. Select *Bridging* from the Options Menu. The following menu will then be displayed:

```
Bridging Menu:

   1) Enable/Disable Bridging
   2) Spanning Tree
   3) Mode of Operation
   4) Bridge Filters
   5) Known Connect List

Select function from above or <RET> for previous menu:
```

2. Select *Enable/Disable Bridging*.

3. Follow the onscreen instructions to complete the configuration.

MAC LAYER BRIDGING CONFIGURATION ELEMENTS

STATUS

The MAC Layer Bridging status is either enabled or disabled. As a default it is enabled.

MAC LAYER BRIDGING BACKGROUND INFORMATION

You are given the option of either enabling or disabling the MAC layer bridging feature. When bridging is enabled, the system bridges data packets to the proper destination, regardless of the network protocols being used. The default configuration is bridging enabled.

Note: If the bridge and the IP options are both enabled, the system will act as a "brouter." A brouter operates as a router for protocols it can route, and operates as a bridge for protocols it cannot route.

CONFIGURING BASIC IP ROUTING

OVERVIEW

This chapter provides information for configuring basic IP routing features. Basic IP routing configuration includes:

- enabling / disabling the Internet Protocol (IP)
  When you enable this option, the system operates as an IP Router. If you also enable bridging, it will route IP packets and bridge all other packet types.
- configuring the IP operating mode
  The operating mode may be either host or router. The router operating mode is the default. The IP host mode allows you to use IP applications, such as Telnet and SNMP, without enabling IP routing.
- configuring network interfaces
  Network Interfaces define the IP networks to which the CyberSWITCH provides access. If IP RIP is enabled, this also includes IP RIP interface information.
- configuring static routes (this includes default routes)
  Other routers on the network that support IP RIP will not need static routes; IP RIP will maintain those routes. However, static routes must be configured to identify remote networks connected across the WAN, and for routers that do not support IP RIP.
- enabling / disabling IP RIP
  IP RIP automates the maintenance of routing tables on IP devices.

A separate chapter, *Configuring Advanced IP Routing*, provides information for configuring advanced IP routing features. Advanced IP routing features include:

- configuring static ARP table entries
- enabling / disabling the isolated mode
- enabling / disabling static route lookup via RADIUS
- configuring the IP address pool
- configuring IP filters
- configuring DHCP
- configuring DNS and NetBIOS addresses
- configuring Security Associations for encryption

INTERNET PROTOCOL (IP) OPTION

ENABLING IP

USING CFGEDIT

1. Internet Protocol (IP) routing is disabled as a default. To begin the IP routing configuration, you must first enable IP routing. Select *IP Routing* from the Options menu.

2. Follow the onscreen instructions for enabling IP routing. Once IP has been enabled, the full IP Configuration menu will be displayed as shown below:

```
IP Configuration Menu:

   1)  IP Routing (Enable/Disable)
   2)  IP Operating Mode
   3)  IP Interfaces
   4)  Static Routes
   5)  RIP (Enable/Disable)
   6)  IP Static ARP Table Entries.
   7)  Isolated mode (Enable/Disable)
   8)  Static Route Lookup via RADIUS (Enable/Disable)
   9)  Change IP Address Pool
   10) IP filters
   11) DHCP
   12) Security Associations

Select function from above or <RET> for previous menu:
```

IP OPTION CONFIGURATION ELEMENTS

IP OPERATIONAL STATUS
You can enable or disable the Internet Protocol (IP) option. The default is disabled.

IP BACKGROUND INFORMATION

When IP is enabled, the system acts as a router, routing IP datagrams based on IP address information. The default configuration is IP disabled.

Note: If the bridge and the IP options are enabled, the CyberSWITCH will act as a brouter. A brouter operates as a router for protocols it can route, and operates as a bridge for protocols it cannot route.

IP OPERATING MODE

The operating mode may be either host or router. The router operating mode is the default. The IP host mode (which allows you to use IP applications, such as Telnet and SNMP, on a bridged network) is a selectable option.

The *Simple Remote Bridging* chapter of the *Examples Guide* provides an example of a simple bridged network that uses the IP host operating mode for the purpose of easy administrative access.

CONFIGURING THE IP OPERATING MODE

USING CFGEDIT

1. Select *IP Operating Mode* from the IP configuration menu.

2. Select either the IP router or IP host operating mode.
   a. If you select IP router, the following menu is displayed:

```
IP Configuration Menu:

   1)  IP Routing (Enable/Disable)
   2)  IP Operating Mode
   3)  IP Interfaces
   4)  Static Routes
   5)  RIP (Enable/Disable)
   6)  IP Static ARP Table Entries
   7)  Isolated Mode (Enable/Disable)
   8)  Static Route Lookup via RADIUS (Enable/Disable)
   9)  IP Address Pool
   10) IP Filter Information
   11) DHCP
   12) Security Associations

Select function from above or <RET> for previous menu:
```

b. If you select the IP host operating mode, an abbreviated IP configuration is displayed:

```
IP Configuration Menu:

   1) IP Routing (Enable/Disable)
   2) IP Operating Mode.
   3) IP Interfaces
   4) Static Routes
   5) RIP (Enable/Disable)
   6) IP Filter Information
   7) DHCP

Select function from above or <RET> for previous menu:
```

Notes: Static ARP entries, isolated mode, static route lookup via RADIUS, and IP address pool capabilities are not available in IP host operating mode. IP operating mode can *not* be set to host unless bridging is enabled. The network interface information required will also be different if the IP host operating mode is configured.

IP Operating Mode Configuration Elements

IP Operating Mode

The IP operating mode may be configured as either router or host. The default is IP router operating mode.

IP Operating Mode Background Information

The *IP router operating mode* provides a broad range of IP routing capabilities, including support for static ARP entries, isolated mode, static route lookup, and IP address pool. IP router operating mode requires each network interface to have a different subnet number assigned to it.

The *IP host operating mode* allows the management of a device using IP applications (such as Telnet and SNMP) while operating as a bridge. IP host mode is useful in situations where segmenting a network into subnets is not desirable, but remote management is required. Bridging must be enabled before IP host mode is enabled. Only one IP address is assignable, and this IP address is not associated with any physical interface. All IP traffic destined for the system is processed

internally, while all other traffic is bridged. With IP host mode, AppleTALK and/or IPX routing may also be enabled.

Off-node authentication servers are available when IP is enabled regardless of the operating mode. With IP host mode, all traffic is considered bridge traffic, so no IP-specific off-node server lookups are performed. These include:

- IP lookup by a next hop IP address or a next hop device name
- Route lookup by a destination IP address

When the IP operating mode is changed from one mode to the other, changes are automatically made to the configuration sensitive to the IP operating mode.

The IP network interfaces in the router mode and the IP network interface in the host mode are internally stored separately, and therefore they are preserved between the mode switching.

IP static routes are not actually sensitive to the IP operating mode, but they are sensitive to IP network interfaces. As a result, changing the IP operating mode (i.e., changing the network interface configuration) may result in invalidating some of the static routes. Be sure to check this. Correct invalid static routes before restarting the system to avoid the deletion of these routes.

IP NETWORK INTERFACES

CONFIGURING INTERFACES

USING CFGEDIT

Note: IP RIP v1 refers to IP RIP Version 1, and IP RIP v2 refers to IP RIP Version 2. IP RIP v1 supports broadcasting, and IP RIP v2 supports multicasting. The CyberSWITCH supports either version. If you are using IP RIP, you need to know what version of IP RIP the other devices using the IP RIP LAN interface supports.

1. Configure all required IP interfaces. If you previously configured the IP operating mode as routing, the interfaces described in steps 2 through 6 are available. If you previously configured the IP operating mode as host, only one interface will be available. That interface type is described in step 7. To begin, select *IP Interfaces* from the IP configuration menu. Select *Add*.

2. For a LAN IP network interface enter the following information. (Note: you may add more than one LAN IP network interface.)
   a. interface name
   b. IP address assigned to this interface
   c. subnet mask
   d. LAN port number
   e. packet encapsulation type
   f. MTU size
   g. enable/disable Proxy ARP feature
   h. transmit broadcast address
   i. input/output filter name

   If IP RIP is enabled, enter the following additional information:

   j. IP RIP send control
   k. IP RIP respond control

l. IP RIP receive control
m. IP RIP v2 authentication control
n. IP RIP v2 authentication key (required only if the IP RIP v2 authentication control has been configured with a value other than "No Authentication"

Note: With the Secondary IP Addressing feature, you may add more than one LAN network interface. Upon adding a second LAN interface, you must provide a unique interface name and address. You will also need to specify whether this new interface is to be the primary or secondary LAN network interface. Refer to *Multiple IP Addresses* in the Background Information for usage details.

3. For a WAN IP network interface enter the following information:
   a. interface name
   b. IP address assigned to this interface
   c. subnet mask
   d. MTU size
   e. transmit broadcast address

   Note: If this interface uses RIP over a dedicated connection, select "Specific Explicitly" for the transmit broadcast address. You will then enter one address. This is because the system can only exchange RIP packets with one device over this type of connection. Refer to *IP RIP over Dedicated Connections* for more information.

   If IP RIP is enabled, enter the following additional information:

   f. the transmit broadcast IP address (requested if you selected "Specify Explicitly" for the transmit broadcast address)
   g. IP RIP host routes propagation scheme
   h. RIP send control
   i. RIP receive control
   j. RIP respond control
   k. IP RIP v2 authentication control
   l. IP RIP v2 authentication key (required only if the IP RIP v2 authentication control has been configured with a value other than "No Authentication"

4. For a WAN (Direct Host) IP network interface enter the following information:
   a. Direct Host interface name
   b. associated LAN interface
   c. MTU size

5. For a WAN (RLAN) IP network interface enter the following information:
   a. interface name
   b. IP address assigned to this interface
   c. subnet mask
   d. packet encapsulation type
   e. MTU size
   f. enable / disable Proxy ARP feature
   g. transmit broadcast address

If IP RIP is enabled, enter the following additional information:

h. IP RIP send control
i. IP RIP respond control
j. IP RIP receive control
k. IP RIP v2 authentication control
l. IP RIP v2 authentication key (required only if the IP RIP v2 authentication control has been configured with a value other than “No Authentication”

6. For a WAN IP UnNumbered network interface enter the following information:
   a. MTU size

7. For a system configured in the IP host operating mode, the following information will be required for a network interface:
   a. IP address assigned to this interface
   b. subnet mask
   c. MTU size
   d. transmit broadcast address

   If IP RIP is enabled, enter the following additional information:

   e. IP RIP receive control
   f. IP RIP respond control
   g. IP RIP v2 authentication control
   h. IP RIP v2 authentication key (required only if the IP RIP v2 authentication control has been configured with a value other than “No Authentication”

USING MANAGE MODE COMMANDS

ipnetif
This command displays the current IP network interface configuration.

NETWORK INTERFACE CONFIGURATION ELEMENTS

TYPE
Specifies the interface type: LAN, WAN, WAN Direct Host, WAN RLAN (Remote LAN), or WAN UnNumbered. For the LAN, you may configure both primary and secondary interfaces. The primary interface specifies how RIP, IP filters, and proxy ARP operate on all LAN network interfaces for a specified LAN port.

NAME
User-defined. An interface name is a 1 to 16 character user-defined string that identifies the interface to the system administrator. Each interface (LAN or WAN) must have a unique name.

IP ADDRESS
The IP address (using dotted decimal notation) assigned to this interface. The IP address applies to LAN type interfaces and WAN type interfaces only. Each LAN interface must be configured with a unique IP address.

SUBNET MASK
The Subnet Mask value (the number of significant bits for the subnet mask) associated with the IP address specified for this interface. The Subnet mask is specified by entering the number of contiguous bits that are set for the mask. The mask bits start at the most significant bit of the IP address field and proceed to the least significant bit. Subnet Mask applies to LAN, WAN, and WAN RLAN type interfaces only. WAN Direct Host network interfaces use the subnet mask from the associated LAN network interface.

PORT
If the interface type is LAN, then this indicates the port number on the Ethernet-2 resource to which the physical LAN for this interface is connected. The LAN port can support multiple network interfaces.

If the interface type is WAN Direct Host, then this indicates the port number on the Ethernet-2 resource of which this interface is a logical extension.

ENCAPSULATION
If the interface is LAN or WAN RLAN, this specifies the encapsulation type for IP datagrams transferred on this interface. Ethernet type encapsulation specifies that IP datagrams are transferred in standard Ethernet frames as specified in RFC-894. SNAP type encapsulation specifies that IP datagrams are transferred in 802.3 format frames using the Sub Network Access Protocol (SNAP) as specified in RFC-1042.

For multiple LAN network interfaces, you may specify different encapsulations for each.

MTU
This specifies the maximum number of bytes that can be transmitted on the network interface. Some devices on the network may not be able to receive large data packets. This parameter allows you to maintain compatibility with these devices by setting the MTU to agree with that supported by the device. This parameter is a decimal value from 60 to 1500, depending on the type of datagram encapsulation selected.

For multiple LAN network interfaces, you may specify different MTU sizes for each.

PROXY ARP
You may enable or disable proxy ARP for a LAN or RLAN interface. Proxy ARP helps hosts, with no routing knowledge, communicate with hosts on other IP subnets. It works as follows: when a CyberSWITCH receives an ARP request for a host that is not on the same IP subnet as the requester, the CyberSWITCH checks to see if it provides the best route to the remote host. If it does, the CyberSWITCH will reply to this ARP request with its own MAC address. The host that has sent the ARP request then communicates with the remote host by sending packets to the CyberSWITCH. The CyberSWITCH will forward those packets using standard IP routing.

For multiple LAN network interfaces, the setting on the primary network interface also applies to all secondary network interfaces configured for the physical LAN port. You cannot change the proxy ARP setting on secondary network interfaces.

TRANSMIT BROADCAST ADDRESS
Specifies the transmit broadcast address on numbered interfaces (meaning all interfaces except interfaces that have been defined as unnumbered). This information is used by all network applications (protocols) that use broadcasting capabilities. There are five selections available for the transmit broadcast address. The first four selections are produced from the IP address that is

entered for the interface. For example, if the IP address of the interface is 199.120.211.98, the portion of the menu displaying the available transmit broadcast addresses would appear as:

```
Transmit Broadcast Address:
   1) 199.120.211.255
   2) 199.120.211.0
   3) 255.255.255.255
   4) 0.0.0.0
   5) Specify Explicitly

Enter Transmit Broadcast Address [default = 1]? 1
```

In almost all cases, the default transmit address is used (1). The only time any of the other numerical addresses are used is if the default has been configured, and the machines are not responding to IP RIP or some other broadcast protocol. If this happens, try the other Transmit Broadcast Address menu selections. Some older UNIX machines may work with selection (2) or (4). Regardless of which address is selected, the goal is to allow broadcasts from the defined interface to all devices on the local network.

If you plan to exchange IP RIP packets with devices connected over dedicated links or semi-permanent connections, select *Specify Explicitly*. You can then explicitly specify the device (only one) with which the CyberSWITCH will be exchanging packets. You may also select this option to support a unicast address feature for a numbered WAN interface. (See RIP Send Control options.) This will avoid sending packets to all remote devices on the IP network.

TRANSMIT BROADCAST IP ADDRESS
Requested only if you selected *Specify Explicitly* for the transmit broadcast address. The IP address of the device with whom the CyberSWITCH will be exchanging RIP packets.

For multiple LAN network interfaces, you must have an associated transmit broadcast address for each interface.

INPUT / OUTPUT FILTER NAME
A *filter* is a list of conditions which modifies the normal processing flow of packets. You may specify the name of a *predefined input and/or output filter* for the primary interface on a LAN port. All secondary interfaces assigned to the same LAN port are subject to the actions specified by these filters. When configuring a secondary LAN interface, you cannot change the filter information.

RIP INFORMATION
(See individual Send Control, Receive Control, Respond Control and Authentication Control elements). You may configure one set of RIP parameters for the primary network interface on a LAN port. All other secondary interfaces assigned to the same LAN port are subject to the same actions specified by these parameters. When configuring a secondary LAN interface, you cannot change the RIP information.

You may also configure a set of RIP parameters for each RLAN or numbered WAN interface.

IP RIP SEND CONTROL
If IP RIP is enabled for a specific interface (LAN, WAN RLAN, and / or numbered WAN interfaces), an IP RIP send control must be selected. This element controls how IP RIP update messages are sent on an IP RIP interface. There is a different default value depending on the type of interface configured. The default value is automatically preconfigured when IP RIP is enabled.

The following tables provide the possible options for IP RIP send control.

For ***LAN*** and ***WAN RLAN*** interfaces:

Send Control Options	*Description*	*RIP Version Sent*
Do Not Send*	Indicates no IP RIP packets to be sent.	(none)
IP RIP v1**	Compliant with RFC 1058. Uses standard (broadcast) addressing.	RIP v1
IP RIP v1 Compatible	Uses RFC 1058 route subsumption rules with standard (broadcast) addressing	RIP v2
IP RIP v2	Compliant with RFC 1723. Uses standard (multicast) addressing	RIP v2

(*) The default switch for WAN RLAN interface.
(**) The default switch for LAN interfaces.

For ***numbered WAN*** interfaces:

Send Control Options	*Description*	*RIP Version Sent*
Do Not Send*	Indicates no IP RIP packets to be sent.	(none)
IP RIP v1	Compliant with RFC 1058. Use with unicast addressing only (*Specify Explicitly* option).	RIP v1
IP RIP v1 Compatible	Uses RFC 1058 route subsumption rules. Use with unicast addressing only (*Specify Explicitly* option)	RIP v2
IP RIP v2	Compliant with RFC 1723. Uses standard (multicast) addressing	RIP v2

(*) The default switch for numbered WAN interfaces.

IP RIP RESPOND CONTROL
If IP RIP is enabled for a specific interface, then designation of this element is required.
This element controls how the system responds to IP RIP requests on the interface. The default value is automatically preconfigured when IP RIP is enabled.

The following table provides the possible choices for IP RIP respond control.

Switch	*Meaning*
Do Not Respond	This switch indicates responding to no IP RIP requests at all.
IP RIP v1 Only	This switch indicates responding only to IP RIP requests compliant with RFC 1058.
IP RIP v2 Only	This switch indicates responding only to IP RIP v2 requests compliant with RFC 1723.
IP RIP v1 or IP RIP v2 *	This switch indicates responding with the same IP RIP version format as the version of the request.

*The default switch.

IP RIP RECEIVE CONTROL
If IP RIP is enabled for a specific interface, then this element is required.
This controls which version of IP RIP updates are to be accepted. The default value is automatically preconfigured when IP RIP is enabled.

The following table provides the possible choices for IP RIP receive control.

Switch	*Meaning*
Do Not Receive	This switch indicates accepting no IP RIP updates at all.
IP RIP v1 Only	This switch indicates accepting only IP RIP updates compliant with RFC 1058.
IP RIP v2 Only	This switch indicates accepting only IP RIP v2 updates compliant with RFC 1723.
IP RIP v1 or IP RIP v2 *	This switch indicates accepting either IP RIP v1 or IP RIP v2 updates.

* The default switch.

IP RIP v2 AUTHENTICATION CONTROL
If IP RIP is enabled for a specific interface, this element is required.
This controls the type of authentication the CyberSWITCH uses on the interface. The default value is automatically preconfigured when IP RIP is enabled.

The following table provides the possible choices for IP RIP v2 authentication control

Type	*Meaning*
No Authentication *	This control type indicates that IP RIP v1 and unauthenticated IP RIP v2 messages are accepted.
Simple Password	This control type indicates that IP RIP v1 messages and IP RIP v2 messages which pass authentication test are accepted. The authentication test is done using a simple password.

* This is the default switch.

IP RIP v2 AUTHENTICATION KEY
If IP RIP is enabled for a specific interface, this key is required if the following condition has been met: the "IP RIP v2 Authentication Control" has been configured with a value other than "No Authentication." The authentication key is a user-defined password, 1-16 characters in length.

IP RIP HOST ROUTES PROPAGATION SCHEME
If RIP is enabled for a WAN interface, this is required. This controls how the IP RIP packets will be propagated. The default value is "Host Routes Propagation is currently DISABLED." With the default, WAN local routes are propagated as subnetwork routes. If Host routes propagation is enabled, host routes will be propagated on other network interfaces only while each remote IP device is connected to the CyberSWITCH.

When the IP RIP host propagation scheme is enabled, it will allow multiple systems on the same LAN to work properly. IP RIP information is then advertised as multiple host routes as they connect to the CyberSWITCH.

For more information, refer to the diagrams and explanation provided on WAN interfaces beginning on page 145.

IP NETWORK INTERFACE BACKGROUND INFORMATION

Network Interface is a term used to represent the physical connection of the system to a data network. For example, the Ethernet resource provides a network interface to an Ethernet LAN. The ISDN lines provide network interfaces to multiple remote networks. Because of their switched nature, the ISDN lines provide virtual network interfaces. That is, the same physical ISDN line can actually connect to different remote networks by dialing a different phone number.

A bridge device refers to its network interfaces as ports. It simply forwards packets from one port to another without looking at the network protocol information. A typical ISDN bridge has one Ethernet port and one ISDN port.

In a network that uses the IP protocol for communication, a flexible network interface structure can be implemented. An IP network uses the IP network address as a basis for device communication. IP networks can be segmented into a hierarchical structure by using the subnet addressing provided by the IP protocol. IP hosts can be assigned to a specific subnet based on management and user needs. All IP hosts connected to a virtual or physical subnet must have the same subnet address.

An IP Host device has only one network interface that it uses for data transfer. This network interface is assigned an IP address and belongs to one subnet. A remote IP host typically uses an ISDN line for this network interface. All data is sent through this network interface.

An IP router device can have multiple network interfaces. Each of these are assigned an IP address and belong to a separate subnet. The IP router looks at the IP network information in a packet and uses this to decide to which network interface the packet should be forwarded.

The CyberSWITCH provides a set of network interfaces that give you a wide range of flexibility. The network interfaces provided are:

- LAN IP Network Interface
- WAN IP Network Interface
- WAN (Direct Host) IP Network Interface
- WAN (RLAN) IP Network Interface
- WAN (UnNumbered) IP Network Interface

With IP routing enabled, you must specify each network interface and its associated subnet information. This allows the System to route IP data between network interfaces. In this mode, IP Hosts and IP routers can connect to the system. Even MAC layer bridge devices can connect to the system and use IP protocols through a IP RLAN Network Interface.

With the LAN, WAN and WAN(RLAN) IP interfaces, you may enable the Routing Information Protocol (RIP). If RIP is enabled (automatically enabled with new installs; not enabled in upgrades), there will be extra information required for configuring LAN type interfaces (LAN and RLAN interfaces) and WAN interfaces. This is because IP RIP uses these types of interfaces to propagate IP RIP packets. For further information, refer to the section *IP RIP and the IP Network Interfaces*.

The following table provides the IP Network Interfaces and the associated remote devices that use these interfaces.

IP Network Interface Type	*Associated Remote Device*
WAN	IP Host (RFC1294) PPP
WAN (Direct Host)	IP Host (RFC1294) PPP
WAN (RLAN)	HDLC Bridge PPP
WAN UnNumbered	PPP

The *LAN IP Network Interface* is used to define the subnet information for an Ethernet port. This subnet is usually connected to the central IP network. You must configure a LAN IP Network Interface if you have any devices that need to communicate over the local network. You may optionally configure additional secondary LAN IP network interfaces on the same LAN port. Refer to *Network Flattening* for more information.

The *WAN IP Network Interface* is used to define remote IP devices (hosts or routers) that require access to the central network. This network interface represents a different subnet than that connected to a LAN network interface. The WAN IP Network Interface is used for both IP Host and PPP remote devices.

The *WAN (Direct Host) IP Network Interface* allows you to extend the LAN subnet to remote devices. The WAN (Direct Host) IP Network Interface is used for IP Host and PPP remote devices. When configuring a WAN (Direct Host) interface, you must specify the Direct Host interface name and its associated LAN interface. You may also specify filters and DHCP proxy client information for this interface type. Note that the RIP feature is not supported for this interface.

The *RLAN (Remote LAN) IP Network Interface* allows remote MAC layer bridge devices to connect to an IP subnet. The CyberSWITCH treats all devices connected to the RLAN Network Interface as if they were connected to the same Ethernet segment. The system provides an explicit IP router presence on this RLAN that is implemented over ISDN. IP Address Resolution requests are intelligently propagated to remote bridged networks connected on the RLAN network interface. The WAN RLAN Network Interface is used for HDLC Bridge and PPP remote devices.

The *WAN (UnNumbered) Interface* allows you to configure an IP WAN interface without assigning an IP address to it. With this feature, unnecessary logical IP sub-network numbers for the WAN connections do not have to be created; therefore, IP sub-network numbers can be saved. Note that if a WAN (UnNumbered) Interface is configured, you must first add any devices that will be used as next hop devices (for static routes), before you can configure the static routes themselves. This is because you will need to enter the device's name for the next hop device, and you will not be allowed to do this if you have not already configured the device.

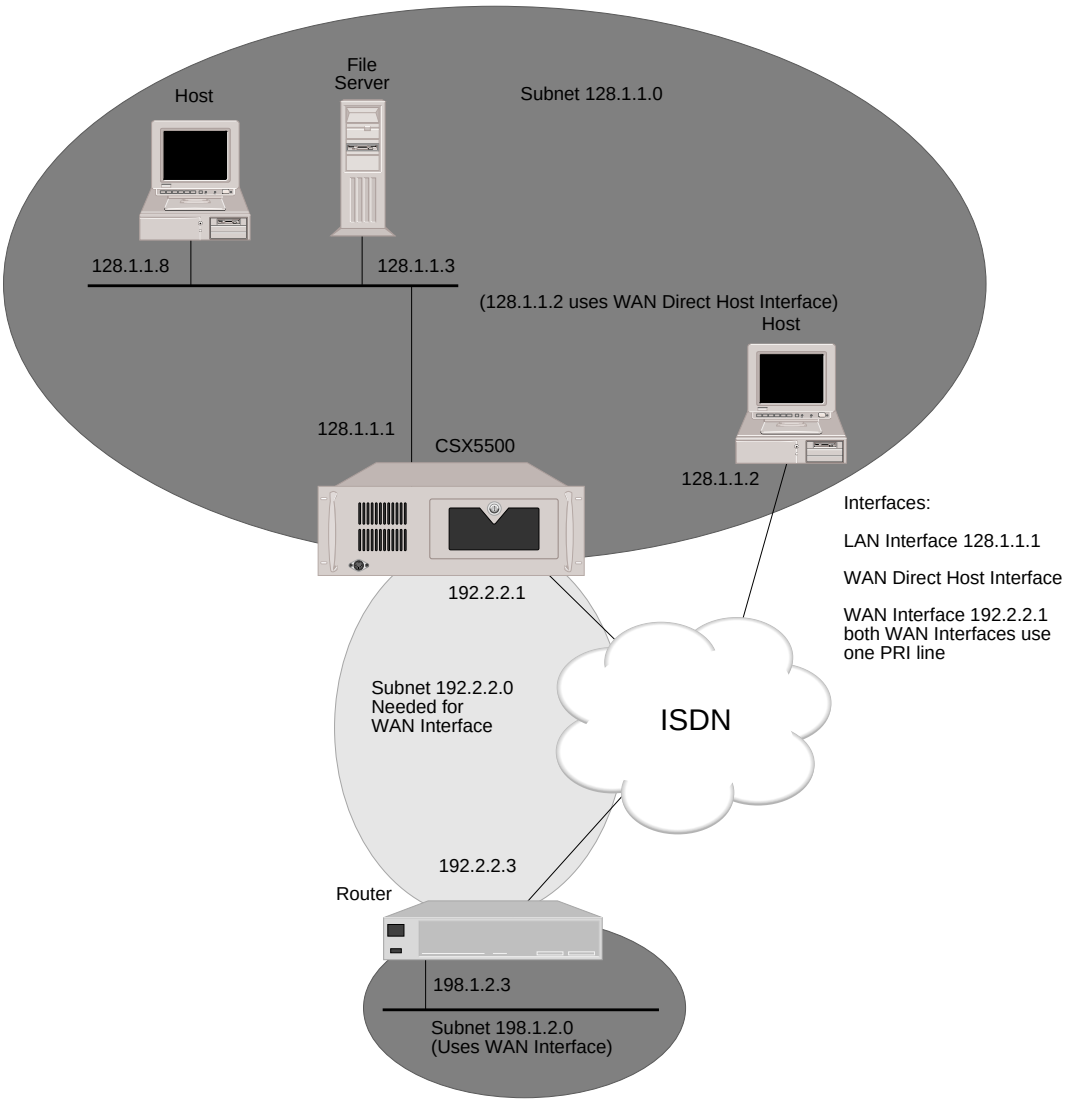
The UnNumbered Network Interface allows you to configure an IP WAN Interface without assigning an IP address to it (for PPP devices only). Unnecessary logical IP (sub-) network numbers can be saved. The *Quick Start's* section regarding *CyberSWITCH Connectivity via PPP* illustrates the associated steps needed to set up an UnNumbered Interface for PPP devices.

Basically, for each PPP device that shares the UnNumbered interface, you must:

- Configure an IP LAN Network Interface (if not already configured).
- Add a WAN UnNumbered Interface (if not already configured).
- Skip ahead to the main menu Security selection (3), and add the device that will be used as the next hop device. You must do this because to add the static route for an UnNumbered interface, you need to enter another system's (a device's) name for the next hop device. To do this, you must already have a device configured.
- When entering the device list information for the system that will act as the next hop, enter 0.0.0.0 as the device's IP address because this is an UnNumbered network interface.
- Return to the options configuration and add a static route to the other system(s) sharing the Un-Numbered Interface, using the other system's name as the next hop device.

Note: The RIP feature is not supported for UnNumbered WAN Interfaces.

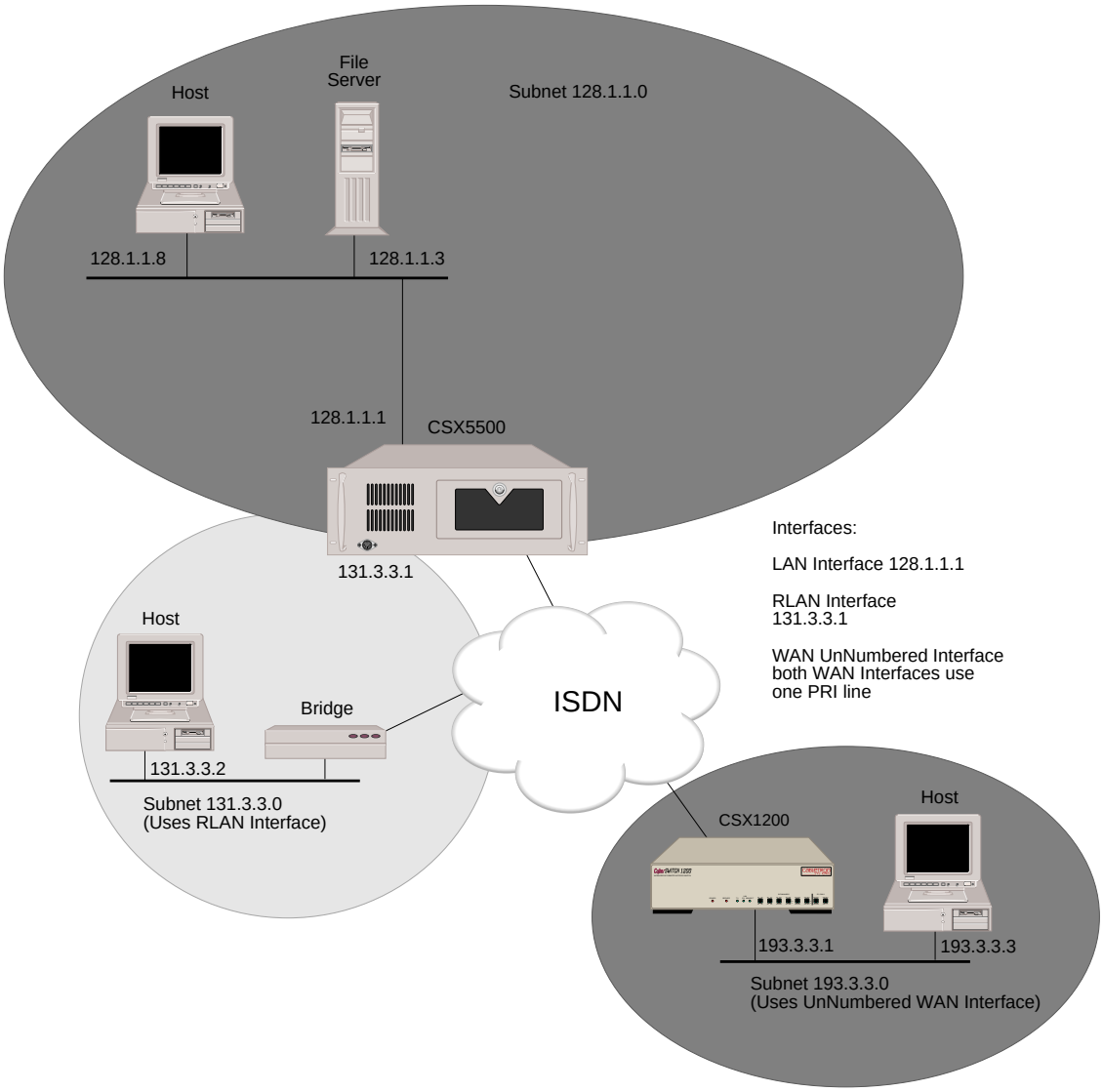
The following diagrams provide examples of each interface type. The variety of network interfaces available allows you to install a wider range of devices at the remote sites.



Example 1: LAN, WAN and WAN Direct Host Interfaces

In example 1, we show three different types of network interfaces and the IP subnets that are used. It should be noted that even though the CyberSWITCH only has one physical connection to the WAN, it has more than one logical connection. Also, each one of these logical interfaces can be in different subnetworks.

- The LAN interface is the simplest. It specifies the IP address (128.1.1.1) which connects the system to the Ethernet LAN. In our example, only one LAN interface is configured.
- The Direct Host interface doesn't have an IP address. Devices that use the Direct Host interface must have an IP address that is on the same subnet as one of the configured LAN interfaces. Since only one LAN interface is configured, that IP address must correspond to the one configured LAN IP address. (See *Secondary IP Addressing* for multiple LAN IP addresses).
- The WAN interface in this example is used to connect two IP subnets (128.1.1.0 and 198.1.2.0). A separate subnet (192.2.2.0) is required to connect the subnets. If the remote router supports unnumbered interfaces (such as Example 2), then the connecting subnet would not be required.



Example 2: LAN, WAN UnNumbered, WAN Remote LAN Interfaces

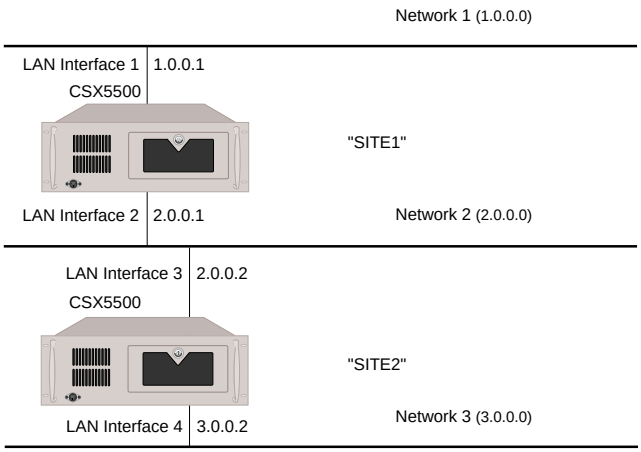
In example 2, the WAN UnNumbered interface is used to eliminate an unnecessary IP Subnet. The RLAN interface is unique in that it extends the IP network over the WAN to remote devices which access the network using a bridge device. Thus it makes a simple bridge device appear to be an IP router. This is accomplished by having the system extend its Ethernet to handle the ARPs for the remote bridge.

IP RIP AND THE IP NETWORK INTERFACES

Routing Information Protocol (RIP) is a protocol used to exchange routing information among IP devices. Using IP RIP can automate the maintenance of routing tables on IP devices and relieve you of having to keep the routing tables up to date manually. IP RIP determines the shortest path between two points on a network in terms of the number of “hops” between those points.

LAN type interfaces (LAN and RLAN Interfaces) and WAN interfaces are used by devices to advertise the IP RIP information. The type of interface used for IP RIP depends on the network configuration. Different interface information must be configured depending on the type of interface used to propagate the IP RIP information.

Devices used to directly connect two LANs use a LAN interface for IP RIP information propagation. The example network shown below illustrates this type of network.

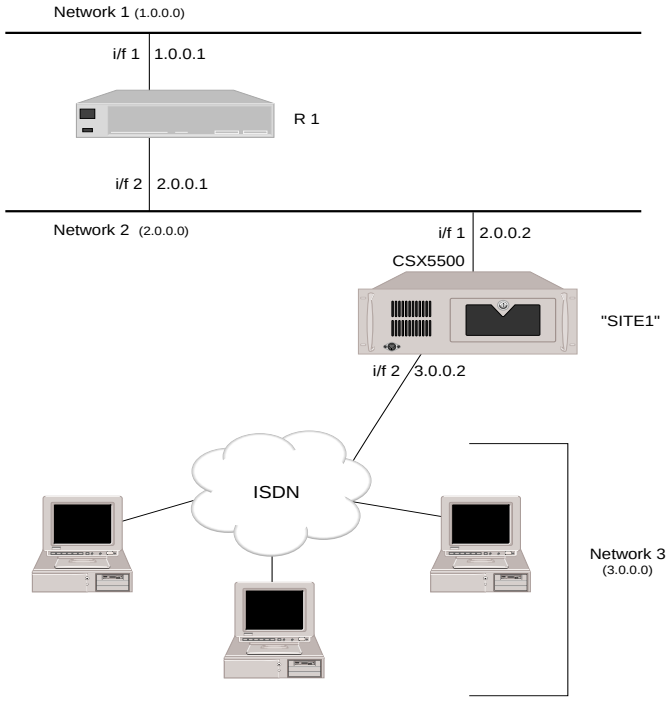


In the above example, both systems (SITE1 and SITE2) need no static routes. SITE1 will learn about Network 3 that can be reached via SITE2 by listening to the IP RIP advertisements from SITE2. SITE2 will also learn about Network 1 in the same way. After learning this route information, the routing tables on SITE1 and SITE2 are updated. Basically, RLAN IP RIP interfaces function in the same manner.

For both LAN type interfaces to function properly with IP RIP, additional LAN interface information is configured. The additional information includes: IP RIP Send Control, IP RIP Respond Control, IP RIP Receive Control, IP RIP v2 Authentication Type, and IP RIP v2 Authentication key. The definitions of these configuration elements are included in the section *Network Interface Configuration Elements*.

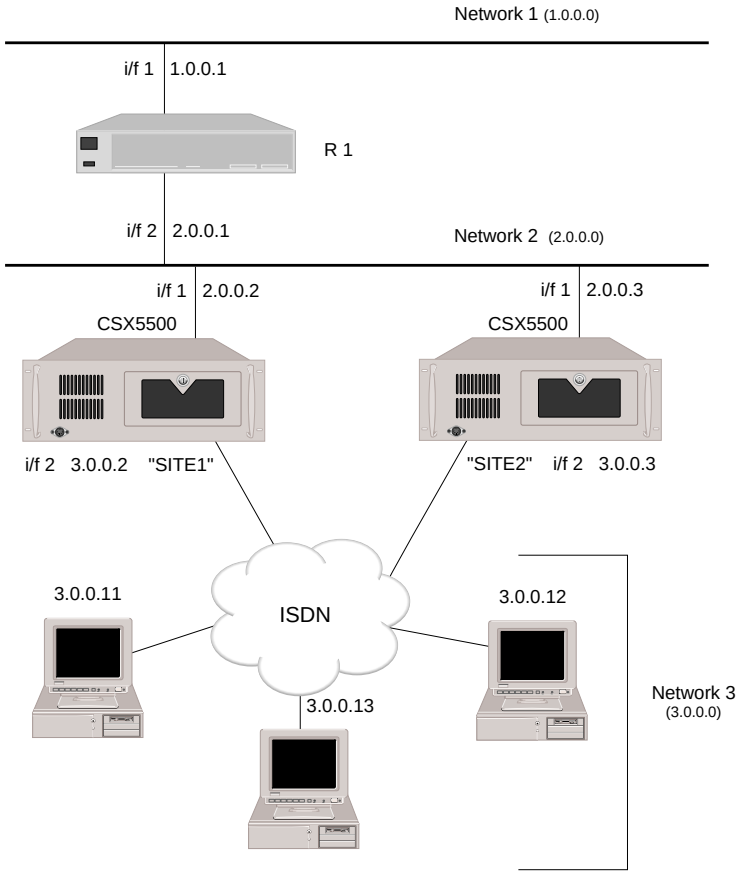
Devices used to connect a logical network to another network use a WAN interface for IP RIP advertisements. Example networks follow which illustrate the different types of networks that would use an IP RIP WAN interface.

See illustration, Example 1. Because SITE1 is the only CyberSWITCH that is connected to the logical network, it is reasonable for SITE1 to advertise the IP RIP information on Network 3 as subnetwork routes, meaning that SITE1 will always advertise the remote IP devices' IP RIP information.



WAN RIP Interfaces: Example 1

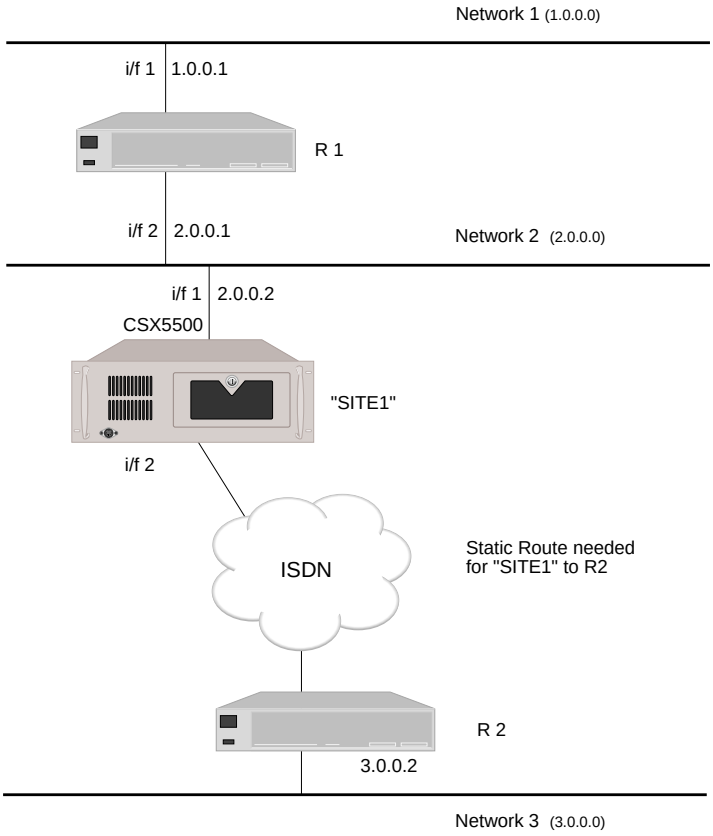
Suppose there is a second CyberSWITCH that belongs to the logical Network 3, as shown in Example 2. It is better for SITE1 and SITE2 to advertise the IP RIP information for each of the remote devices on the logical network on each IP Host device as it connects to the system.



WAN RIP Interfaces: Example 2

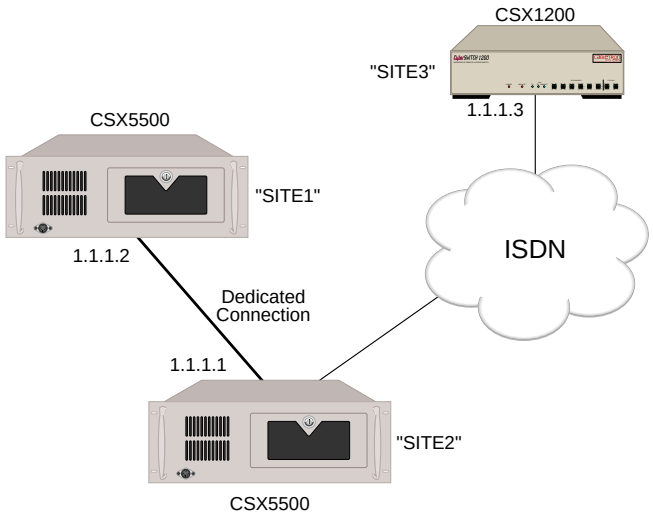
For the WAN interface to function properly with IP RIP, additional WAN interface information is configured. The additional information required involves selecting one of the following: disabling host routes propagation (needed for Example 1), or enabling host routes propagation (needed for Example 2). The definition of this configuration element is included in the section *Network Interface Configuration Elements*.

Currently, IP RIP is not supported across an UnNumbered WAN interface. For example, in the following network setup, SITE1 could not advertise IP RIP information across the UnNumbered WAN IP Interface to Router 2 (R2). Therefore, SITE1 would know about Networks 1 and 2, but would not learn anything about Network 3. In this situation, a static route would have to be configured on the CyberSWITCH. For information on the configuration of static routes, refer to *Static Routes*.

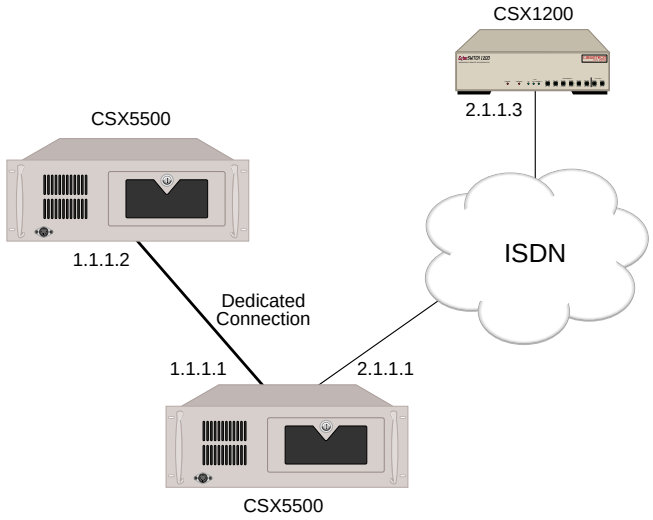


IP RIP over Dedicated Connections

IP RIP is supported over LAN, Remote LAN, and numbered WAN interfaces. When devices are connected over WAN links in which cost is not a major concern, such as dedicated links and semi-permanent connections, RIP can be used to provide dynamic IP routing capability, as illustrated in the following example:



Because each IP WAN network interface on the CyberSWITCH is configured for a logical IP network, various types of physical interfaces (such as V.35 and ISDN BRI) may belong to the same IP network interface. To avoid sending broadcast packets to all remote devices on an IP network, you explicitly specify with which device (only one) the system should exchange RIP packets.
In the previous graphic, the WAN network interface 1.1.1.1 on SITE1 is used to connect to a dedicated line and an ISDN line. You need to specify to which remote device, either SITE2 or SITE3, SITE1 should exchange RIP packets. If it is necessary to run the RIP between SITE1 and SITE3 as well as between SITE1 and SITE2, then another WAN network interface (for example, 2.1.1.1 on SITE1 and 2.1.1.3 on SITE3) must be configured, as illustrated:



IP HOST OPERATING MODE AND THE IP NETWORK INTERFACES

Only one network interface can be configured when the IP operating mode is host. The network interface configuration is not much different from the others available in router mode except that the following configuration items will not be asked:

- Network Interface Type
- Network Interface Name
- IP RIP Send Control

USING MULTIPLE IP ADDRESSES

You may use multiple IP addressing for system backup and / or network flattening implementations. A discussion of both follows.

Redundant Configurations for Backup

To implement a backup system, you will need two CyberSWITCHs with redundant configurations and a Connection Services Manager (CSM).

LAN interfaces on the CyberSWITCH will have primary LAN and IP addresses and may optionally have one or more secondary MAC and IP addresses. You can dynamically add secondary MAC and IP addresses under the control of the CSM workstation.

Typically, you would use primary MAC and IP addresses when transmitting datagrams directly to a particular CyberSWITCH node, and secondary MAC and IP addresses when transmitting datagrams through the CyberSWITCH to other nodes. You would then use CSM to monitor identically configured CyberSWITCH nodes on the same LAN. Should CSM notice some condition which prevents one of the CyberSWITCH nodes from properly performing its function (for example, "link down"), it will order the other CyberSWITCH node to take over the faulty node's duties. The other CyberSWITCH node does so by taking on the identity (the MAC and IP addresses) of the faulty node.

Network Flattening

With IP networks, the total number of available IP addresses is a finite number, and that number is rapidly diminishing. Hosts are typically assigned static addresses; they generally require extensive local configuration in order to operate properly within their defined networks. To allow the IP networks to become more easily and efficiently manageable, we suggest a network flattening approach. Network flattening is a concept which can:

- remove the address hierarchy from the network, and
- remove the requirements that all end nodes need to know the topology of the network (or the address of the default router) to which they attach.

With network flattening, you may draw IP addresses for new nodes from remaining address space from attached subnets. This more efficiently uses the network's address space, since multiple subnets may coexist on the same physical network. The following features help implement the concept of network flattening:

- *Proxy ARP*
  Hosts on flattened networks believe that any host they wish to reach is on a network directly attached to them. When a local device on a flattened network is attempting to communicate

with a remote device on a different subnet, the local device will ARP for the remote host's MAC address.

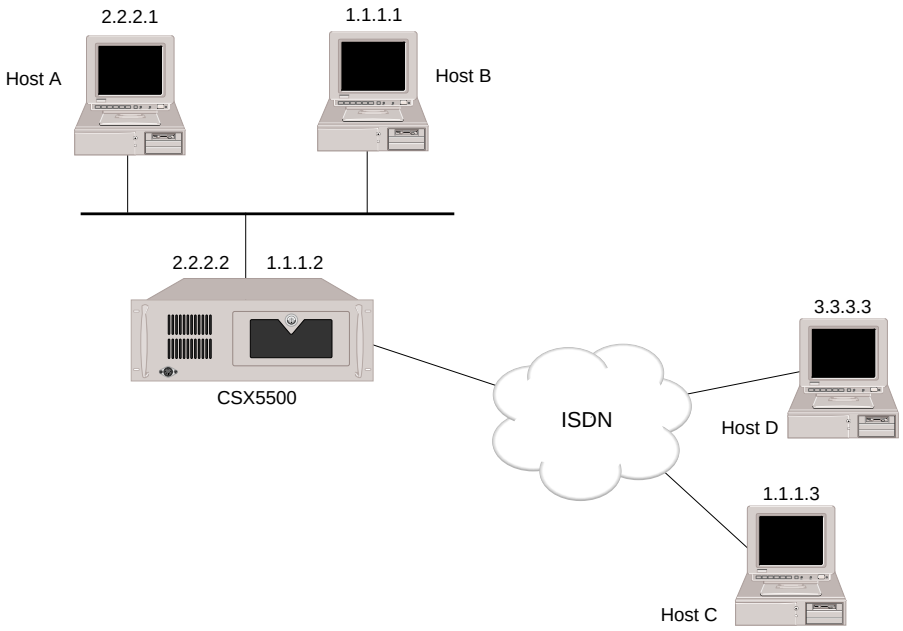
Since routers do not forward ARP requests across subnets, ARPs sent for hosts which are not on the same physical network segment will go unanswered. The proxy ARP feature will potentially generate an ARP reply for remote hosts. If the CyberSWITCH determines that it provides the best route to the remote device, it will respond with an ARP reply containing the MAC address of the CyberSWITCH. Further communication between the two hosts will then be routed through the CyberSWITCH.

- *Secondary IP Addressing*
  If only one IP network interface (i.e., one subnet) per LAN port is configured, any traffic from hosts on different subnets attached to the LAN port would be dropped.

  With the secondary IP addressing feature, multiple IP network interfaces may be configured for each LAN port. All existing subnets which are to be reached will have an associated IP network interface on the CyberSWITCH. By allowing each LAN port to be configured with multiple IP network interfaces, the CyberSWITCH can route packets from hosts on any of the subnets attached to the LAN port. (See following example.)

Example: IP Host Communications in Flattened Networks

To communicate with destination hosts which are not on the same physical wire, you must have a router attached to the edge of the flattened network which can forward packets to those destination networks. In the following illustration, we are using a CyberSWITCH as our "edge" router:



When a local host ARPs for a remote host, the CyberSWITCH (with Proxy ARP enabled) determines if it provides the best route to the destination. If it does, it will reply to the ARP request with its own MAC address.

- *Suppose Host A wishes to contact Host D*. Since Host A thinks every other host is local, it will broadcast an ARP request. The CyberSWITCH, which is on the same physical wire as Host A, will receive the ARP request on one of its LAN network interfaces. The CyberSWITCH makes the determination that it provides the best route to Host D, and generates an ARP response containing its own MAC address. Host A then communicates with Host D by sending packets to the CyberSWITCH edge router. The CyberSWITCH forwards packets to the remote destination using standard IP routing.

- *Suppose Host B wishes to contact Host C*. Host B broadcasts an ARP request. The CyberSWITCH knows that Host C is reachable over a WAN (Direct Host) interface; Host C is considered a logical extension of network 1.x.x.x. The CyberSWITCH generates an ARP response, containing its own MAC address. Host B then communicates with Host C by sending packets to the CyberSWITCH. The CyberSWITCH forwards the packets over the WAN to Host C.

STATIC ROUTES

CONFIGURING STATIC ROUTES

You only need to configure Static Routing entries if you need to access a WAN network that is not directly connected to the system, or if you need to access a LAN network through a router that does not support IP RIP. Static Routes specify the IP address of the next hop router or gateway that provides access to this network.

USING CFGEDIT

1. Select *Static Routes* from the IP menu.

2. When asked if this is a default route, answer "N" for no (for a definition of default routes, refer to *Configuring Default Routes*).

3. Enter the destination address of the designation (sub-) network or host.

4. Enter the subnet mask.

5. Enter the next hop address of the next hop gateway that provides access to the target (sub-) network or host.

6. Enter the metric value (usually the number of routers between the CyberSWITCH and the destination.

7. Enter the IP RIP propagation control (determines how a static route is propagated via IP RIP).

USING MANAGE MODE COMMANDS

iproute

Displays the current IP static routing configuration data. The meaning of each displayed field for a route entry is:

DESTINATION
IP address for the destination network or host.

SUBNET-MASK
Subnet mask value for the destination network or host. A value of 255.255.255.255 indicates that this entry is for a specific IP host.

NEXT HOP
IP address or device name for the next hop router that provides access to the destination network or the host.

METRIC
Hop count to the destination network or the host.

iproute add

Allows an IP static route to be added to the current configuration. The required configuration elements are explained below:

IS THIS THE DEFAULT ROUTE?
Select whether or not this route is the default route or a route to a specific network that has been previously configured. The default route is a form of a static route that is useful when there are a large number of networks that can be accessed through a gateway. Care must be taken when specifying a default route. All IP datagrams that specify a destination IP address that do not have an explicit routing table entry will be sent to the default route. If this destination IP address is unreachable, it could result in a large amount of unnecessary network traffic.

IP-ADDRESS
The Destination IP address using dotted decimal notation. 000.000.000.000 is used to specify the default route coupled with Subnet-Mask value 000.000.000.000.

SUBNET-MASK
The number of significant bits for the subnet mask using dotted decimal notation. The mask bits start at the most significant bit of the IP address field and proceed to the least significant bit. If this is a host specific route entry, the mask value must be 255.255.255.255. Use the default if you are unsure of this value.

NEXT HOP
IP address using dotted decimal notation for the next hop router that provides access to the network or the host specified by IP address. Next hop should be on the network directly connected to a LAN interface or one of the CyberSWITCH IP sites. If next hop is one of the system's IP sites, the IP address for that site should be used.

METRIC VALUE
Hop count to the destination network or the host.

IP RIP PROPAGATION CONTROL
The IP RIP propagation control determines how a static route is propagated via IP RIP. The following table provides an explanation of how a IP RIP propagation control flag is assigned to a static route.

Flag	*Meaning*
Propagate Always	This flag indicates that the route information is always propagated via IP RIP. This flag is available when the next hop is over a LAN or a WAN interface.
Propagate only when the Next Hop is Connected	This flag indicates that the route information is propagated via IP RIP only when the next hop router is connected to the system. This flag is available when the next hop is over a LAN or a WAN interface.
Do Not Propagate	This flag indicates that the static route information is not propagated over the interface. This flag is available only when the next hop is over a WAN interface.

`iproute change`
Allows an existing IP static route to be changed.

`iproute delete`
Allows an IP static route to be deleted from the current configuration.

STATIC ROUTE CONFIGURATION ELEMENTS

DESTINATION IP ADDRESS
IP address using dotted decimal notation that specifies the destination (sub-) network or host.

SUBNET MASK
The Subnet mask for the destination (sub-) network. A subnet mask of 255.255.255.255 implies that this static route entry is for a host rather than a (sub-) network. The Subnet mask is specified by entering the number of contiguous bits that are set for the mask. The mask bits start at the most significant bit of the IP address field and proceed to the least significant bit.

NEXT HOP ADDRESS
IP address using dotted decimal notation (or if an unnumbered WAN interface is used, this configuration element is the device name) for the next hop gateway that provides access to the target (sub-) network or host. The IP address (or the device name) of the Next Hop must be on the (sub) network connected to a defined interface.

METRIC VALUE
The administrative distance to the destination of the entry. The administrative distance is typically measured by the number of hop counts (number of routers) between the CyberSWITCH and the destination, but it is up to you to assign proper value to each route entry. If multiple routes exist to the same destination, the route with the least metric value will be chosen as its primary route. Care must be taken when assigning the metric value of 0, because it is interpreted that the destination is

reachable directly and therefore no intermediate router will be used. The default metric value is 2. The range of metric values for static routes is from 0 to 15.

You may manipulate the metric value to promote a certain default route, or to impede a default route from being used. For example, if there is a route that in reality has several hops, but they are all over LAN connections, you may want to assign a low metric to this route so that a route is taken that is local, thus, no toll charges. Or, perhaps there is a route with a low number of hops, but the connection is over a WAN. You may want to assign this route a high number of hops to limit toll charges, in case there is a local route that could be used.

IP RIP PROPAGATION CONTROL

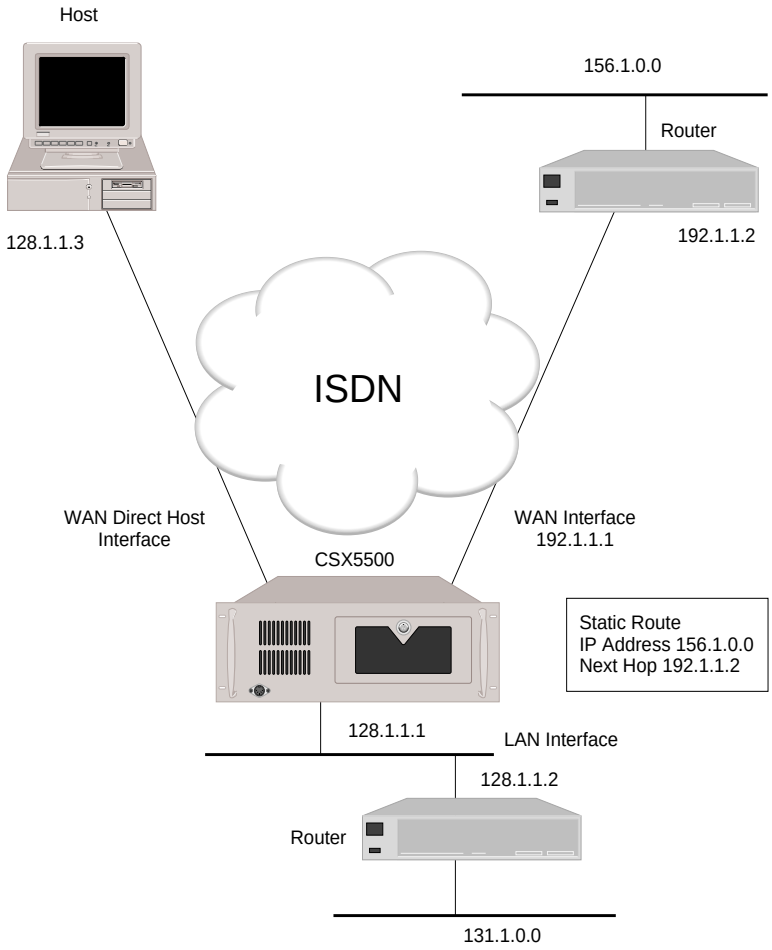
This controls how a static route is propagated via IP RIP. The following table provides an explanation of how a IP RIP propagation control flag can be assigned to a static route.

Flag	*Meaning*
Propagate Always	This flag indicates that the route information is always propagated via IP RIP. This flag is available when the next hop is over a LAN or a WAN interface.
Propagate only when the Next Hop is Connected	This flag indicates that the route information is propagated via IP RIP only when the next hop router is connected to the system. This flag is available when the next hop is over a LAN or a WAN interface.
Do Not Propagate	This flag indicates that the static route information is not propagated over the interface. This flag is available only when the next hop is over a WAN interface.

STATIC ROUTE BACKGROUND INFORMATION

You only need to configure Static Routing entries if you need to access a WAN network that is not directly connected to the system, or if you need to access a LAN network through a router that does not support IP RIP. Static Routes specify the IP address of the next hop router or gateway that provides access to this network.

The following diagram gives an example of a static route definition.



In the above diagram, the Static Route entry indicates that access to IP Network 156.1.0.0 is available through the external router at 192.1.1.2.

A static route is not needed for the CyberSWITCH to access WAN Direct Host 128.1.1.3. Because these two devices are directly connected, (note that the IP addresses are on the same subnet), that route will automatically be established through the system's IP RIP capabilities.

A static route is not needed for system access to IP network 131.1.0.0 through 128.1.1.2 because that route will also be automatically established through the system's IP RIP capabilities.

DEFAULT ROUTES

CONFIGURING DEFAULT ROUTES

The default route is a form of static route that is useful when there are a large number of networks that can be accessed through a gateway. However, care must be taken when specifying a default route. All IP datagrams with a destination IP address that do have an explicit routing table entry will be sent to the default route. If this destination IP address is unreachable, it could result in a large amount of unnecessary network traffic.

USING CFGEDIT

1. Select *Static Routes* from the IP menu.

2. When asked if this is a default route, answer "Y" for yes (for a definition of non-default routes, refer to *Configuring Static Routes*).

3. Enter the next hop address of the next hop gateway that provides access to the target (sub-) network or host.

4. Enter the metric value (usually the number of routers between the CyberSWITCH and the destination.

5. Enter the IP RIP propagation control (determines how a static route is propagated via IP RIP).

USING MANAGE MODE COMMANDS

Refer to the Manage Mode commands used to configure static routes (page 153). Default routes are a subset of static routes. The same Manage Mode commands are used to configure both type of routes.

DEFAULT ROUTE CONFIGURATION ELEMENTS

NEXT HOP ADDRESS
IP address using dotted decimal notation (or if an unnumbered WAN interface is used, this configuration element is the device name) for the next hop gateway that provides access to the target (sub-) network or host. The IP address (or the device name) of the Next Hop must be on the (sub-) network connected to a defined interface.

METRIC VALUE
The administrative distance to the destination of the entry. The administrative distance is typically measured by the number of hop counts (number of routers) between the CyberSWITCH and the destination, but it is up to you to assign proper value to each route entry. If multiple routes exist to the same destination, the route with the least metric value will be chosen as its primary route. The default metric value is 1. The range of metric values for default routes is from 1 to 15.

You may manipulate the metric value to promote a certain default route, or to impede a default route from being used. For example, if there is a route that in reality has several hops, but they are all over LAN connections, you may want to assign a low metric to this route so that a route is taken that is local, thus, no toll charges. Or, perhaps there is a route with a low number of hops, but the

connection is over a WAN. You may want to assign this route a high number of hops to limit toll charges, in case there is a local route that could be used.

IP RIP PROPAGATION CONTROL
This controls how a default route is propagated via IP RIP. The following table provides an explanation of how a IP RIP propagation control flag can be assigned to a default route.

Flag	*Meaning*
Propagate Always	This flag indicates that the route information is always propagated via IP RIP. This flag is available when the next hop is over a LAN or a WAN interface.
Propagate only when the Next Hop is Connected	This flag indicates that the route information is propagated via IP RIP only when the next hop router is connected to the system. This flag is available when the next hop is over a LAN or a WAN interface.
Do Not Propagate	This flag indicates that the static route information is not propagated over the interface. This flag is available only when the next hop is over a WAN interface.

ROUTING INFORMATION PROTOCOL (RIP) OPTION

Routing Information Protocol (RIP) is a protocol used to exchange routing information among IP devices. Using IP RIP can automate the maintenance of routing tables on IP devices and relieve you of keeping the routing tables up to date manually. IP RIP determines the shortest path between two points on a network in terms of the number of "hops" between those points.

ENABLING/DISABLING IP RIP

USING CFGEDIT

1. If you are installing new system software, the IP RIP processing is enabled by default if IP routing has been enabled. Therefore, if you have already enabled IP routing, you do not need to enable IP RIP. If you are upgrading software, the IP RIP processing is not enabled by default; you will need to enable IP RIP.

2. To enable IP RIP:
   a. Return to the IP menu and enable IP routing if you have not already done so.
   b. Select *RIP (Enable/Disable)* from the IP menu, and follow the on-screen instructions for enabling IP RIP.

USING MANAGE MODE COMMANDS

iprip
This command tells you if IP RIP is currently enabled or disabled.

iprip off
If IP RIP is enabled, this command allows you to disable IP RIP.

iprip on
If IP RIP is disabled, this command allows you to enable IP RIP.

IP RIP CONFIGURATION ELEMENTS

IP RIP STATUS
The status IP RIP may be enabled or disabled.

IP RIP BACKGROUND INFORMATION

IP RIP is a protocol used to exchange routing information among IP devices. Using IP RIP can automate the maintenance of routing tables on IP devices and you of manually keeping the routing tables up-to-date. IP RIP determines the shortest path between two points on a network in terms of the number of hops between those points.

If routing is enabled, and IP RIP is enabled, there will be default IP RIP information configured under for LAN type interfaces and WAN interfaces. This configuration information is defined in the section titled *Network Interface Configuration Elements*.

Notes: WAN connection information is propagated on LAN connections. Currently, IP RIP is supported over:

- LAN
- WAN (Remote LAN)
- numbered WAN

RIP is supported over WAN (RLAN) and numbered WAN links regardless of type of telco access (dedicated, semi-permanent dial-up, or normal dial-up). Typically, however, it is enabled over usage-sensitive WAN links, such as dedicated or semi-permanent dial-up.

For a more detailed explanation, refer to *IP RIP and the IP Network Interfaces*.

SECURITY AND ENCRYPTION OPTIONS

The CyberSWITCH product allows you to decide the extent and type of security for your network. This security may consist of standard security options, or it could include data encryption through the purchase of the CyberSWITCH encryption option.

The CyberSWITCH supports standard security options which are independent of the encryption process. These options may or may not be encrypted. These options include: device level security, user level security, a combination of the two, or if preferred, no security. There are different ways to authenticate, as well as different locations (both local and remote) to store security information. This segment addresses these areas.

We include the following chapters in the *Security Configuration* segment of the *User's Guide*:

- *Security Overview*
  The "Big Picture" of how our standard security options work, and how they interoperate.

- *Configuring Security Level*
  Instructions for enabling the level of security you wish to use for security. You may choose to enable no security, device level security, user level security, or both device and user level security.

- *Configuring System Options and Information*
  Instructions for enabling system options, such as PPP Link security, for configuring system information, such as a system password, and for configuring secure yet flexible administration sessions.

- *Configuring Device Level Databases*
  Instructions for configuring an on-node device database (formerly known as the local user list) and enabling an off-node device database. Off-node device databases supported are: Connection Services Manager (CSM) and RADIUS.

- *Configuring User Level Databases*
  Instructions for enabling an off-node database with user level security. User level databases supported are: RADIUS, TACACS, and ACE.

- *Configuring Off-node Server Information*
  Instructions for configuring an off-node server, such as CSM, RADIUS, TACACS, and ACE.

- *Configuring Network Login Information*
  Instructions for configuring general network login information (such as Terminal Server security), network login banners, and information specific to RADIUS and TACACS servers.

In addition to standard security options, the CyberSWITCH encryption option is available. This option provides encryption at either the Network Layer level (using IP Security) or the Link Layer level (using PPP only). The following chapter addresses the set up of this encryption feature:

- *Configuring Encryption*

SECURITY OVERVIEW

OVERVIEW

Security is an important issue to consider when you are setting up a network. The CyberSWITCH provides several security options, and this chapter describes the "Big Picture" of how these options work and interoperate. This information will better equip you to proceed with the following phases of security configuration:

1. configuring the level of security
2. configuring system options and information
3. configuring device level databases
4. configuring user level databases
5. configuring off-node server information
6. configuring network login information

These phases of security configuration are described in detail in the following chapters.

SECURITY LEVEL

The first phase of security configuration is selecting the type of security for your network. The CyberSWITCH offers the following options for Network Security: no security, device level security, user level security, or device and user level security.

If you opt to use no security, for example with a bridged network, no further security configuration is required. No database is needed for this option.

Device level security is an authentication process between internetworking devices. Authentication happens automatically without any human intervention. The devices authenticate each other using a specific authentication protocol, based on preconfigured information. Both bridges and routers support device level security.

If you select device level security for your network, you may specify to use the on-node database, Connection Services Manager (CSM), or RADIUS for the authentication database.

User level security is an authentication process between a specific user and a device. In contrast to the device level security, this authentication process is performed interactively. Interactive user security may use security token cards. Token cards are credit card-sized devices. The system supports a security token card called SecurID, provided by Security Dynamics.

The SecurID card works on a "passcode" concept, which consists of three factors:

- the user's name
- the user's password
- a dynamically-generated value (from the SecurID card)

If you select user level security for your network, you may specify to use RADIUS (with limited capabilities), TACACS, or ACE server.

Multilevel security provides both user level security and device level security for local (on-node) database, Radius, and CSM. This provides added protection; first, a device will be authenticated, and then a particular user (on the device) will be authenticated.

The feature also allows the configuration of an on-node device database at the same time as an off-node device database. Calls first check the on-node database (if enabled) and then the off-node database for the correct device. Authentication is based on device information received from the first matching database.

SYSTEM OPTIONS AND INFORMATION

The second phase of security configuration involves the proper setting of administrative security options. We have thus far defined the selected type of security we plan to use. We now need to enable security options, provide system information, and configure administrative sessions.

System Options: You need to enable / disable PPP Link Security, Bridge MAC Address Security, IP Host ID Security, or Calling Line ID Security, based upon your network requirements.

System Information: You need to assign a system name, password, and secret to the CyberSWITCH for identification purposes.

Administrative Session Information: You can achieve secure administration sessions with flexible control through the configuration of certain options, such as:

- Selecting an authentication database for administration sessions.
  You may select an on-node database, a RADIUS server, a TACAS Server, or an ACE Server.
- Specifying an inactivity session time-out.
  Since there are only a limited number of sessions available, this avoids the problem of administrator lockout because a user forgets to logout from the system.
- Restricting Telnet access.
  This is done by allowing you to set the number of possible administrative Telnet sessions. Telnet access to the CyberSWITCH can be disabled, or the number of Telnet sessions can be limited to less than 3.
- Accessing an emergency Telnet Server session.
  To access an emergency Telnet Server session, you first need to configure an emergency Telnet Server port. If the system administrator needs a Telnet session and all available Telnet sessions are in use, they can then Telnet into this emergency port and disconnect inactive Telnet sessions and begin a session of their own.

DEVICE LEVEL DATABASES

If device level security or multi-level security has been chosen, then the next phase of security configuration involves setting up a device level authentication database, and then specifying the location of that database.

The CyberSWITCH provides dial in / dial out access for remote devices via ISDN connections. The information required to authenticate the remote device is maintained in a database that the system queries during connection establishment. The system allows this "device database" to be located in several optional environments.

These environments include an on-node database and a variety of off-node, central authentication databases. The on-node database contains a list of valid devices that can access the network resources connected to the CyberSWITCH. This list of valid devices is configured and stored locally. A central database allows a network with more than one CyberSWITCH to access one database for device authentication. Supported central authentication databases for device level security include: CSM and RADIUS.

USER LEVEL DATABASES

If user level security or multi-level security has been chosen, then the next phase of security configuration involves enabling an off-node user level authentication database, and then specifying the Telnet port used to access that database. User level security is only available through an off-node authentication server. Servers supported are: RADIUS, TACACS, and ACE.

OFF-NODE SERVER INFORMATION

If an off-node authentication server has been chosen for device or user level security, then the next phase of security configuration requires that these servers are appropriately configured in the system.

CSM is an off-node, central database supported by the CyberSWITCH. CSM is installed on a Windows NT system that is local to the network. It operates with an SQL Server that can store data for thousands of users. A TCP connection allows the CyberSWITCH to communicate with CSM.

The Remote Authentication Dial-In User Service (RADIUS) is a central database supported by the CyberSWITCH. RADIUS operates using two components: an authentication server and client protocols. The RADIUS Server software is installed on a UNIX-based system that is local to the network. The client protocols allow the CyberSWITCH to communicate with the RADIUS server, ultimately authenticating devices.

The Terminal Access Controller Access Control System (TACACS) is a database supported by the CyberSWITCH. TACACS operates using two components: client code and server code. TACACS server software is installed on a UNIX-based system connected to the CyberSWITCH network. The client protocols allow the system to communicate with the TACACS server, ultimately authenticating devices.

Access Control Encryption (ACE) is a database supported by the system. ACE operates using two components: client code and server code. The ACE Server software is installed on a UNIX-based system connected to the network. The client protocols allow the CyberSWITCH to communicate with the ACE Server, ultimately authenticating users.

NETWORK LOGIN INFORMATION

The last phase of security configuration involves configuring network login information. If you are using User Level Security or Multilevel Security, you may customize banners and login configuration to suit the needs of your particular installation. You may also specify the number of login attempts and password change attempts. Specific login elements, such as prompt order, for RADIUS and TACACS are defined here.

CONFIGURING SECURITY LEVEL

OVERVIEW

The CyberSWITCH offers the following levels of network security: no security, device level security, user level security, or device and user level security. The network security level determines the type of security you want activated on your network. As the name implies, no security is used if you configure your network security level as “no security.” Device level security and user level security provide a flexible amount of security, but each secure a different entity:

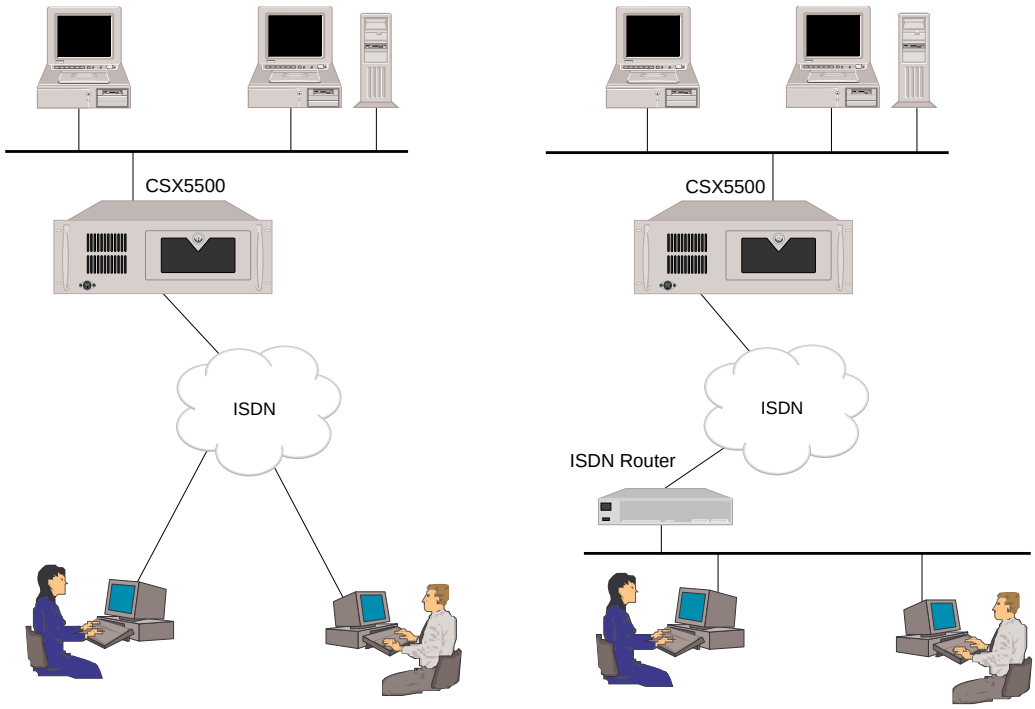
- *Device level security* is an authentication process between internetworking devices. The authentication happens automatically without any human intervention.

- *User level security* is an authentication process between a specific user and a device. In contrast to the device level security, this authentication process is performed interactively.

The combination of both device and user level security supports user authentication on top of device level authentication. Often referred to as multilevel security, this option increases the security on your network. First, authentication takes place at the device level. If the system meets these requirements, then user level security begins by telneting to the appropriate authentication server.

Note: The default value on your initial configuration is device level security, with all security options enabled.

The following picture illustrates two different levels of security. The picture on the left represents User Level Security. The users, not the devices, are authorized before they are allowed access. This would be advantageous, for example, for a user traveling to different areas, using different devices, but still needing access. No matter what device the user is on, the user can be authenticated.The picture on the right represents device level security. The devices are authenticated before access is allowed, no matter who the specific user may be. The device level authentication process is transparent to the user.



Plan what level(s) of security you will use, and configure them now. You will later assign and configure authentication databases to the network security level you configure and to administration sessions. The table below identifies the types of authentication databases that are applicable (specified by yes) for each type of network security and for administration sessions.

Database	*Device Level Security*	*User Level Security*	*Administration Sessions*
On-Node	yes	no	yes
RADIUS	yes	yes	yes
TACACS	no	yes	yes
ACE	no	yes	yes
CSM	yes	no	no

NO SECURITY

CONFIGURING NO SECURITY

USING CFGEDIT

1. To begin the configuration of an on-node database or any of the Security Database options, start at the main menu and progress through the screens as shown below:

```
Main Menu:

   1) Physical Resources
   2) Options
   3) Security
   4) Save Changes

Select function from above or <RET> to exit: 3
```

```
Security Menu:

   1) Security Level
   2) System Options and Information
   3) Device Level Databases
   4) User Level Databases (Enable/Disable)
   5) Off-node Server Information
   6) Network Login Information

Select function from above or <RET> for previous menu: 1
```

2. Select *Security Level* from the Security Menu. The following menu is then displayed:

```
Security Level Menu:

   1) No Security
   2) Device Level Security
   3) User Level Security
   4) Device and User Level Security

Current Security Level is "Device Level Security".

Select function from above or <RET> for previous menu: 1
```

3. Press (1) to change the security level to *No Security*. Follow the onscreen instructions. Note that if you have a previously configured on-node device database, all entries will be lost.

USING MANAGE MODE

seclevel
Displays the current security level configuration data.

DEVICE LEVEL SECURITY

CONFIGURING DEVICE LEVEL SECURITY

USING CFGEDIT

1. Select *Device Level Security* from the Security Level Menu. If you need guidance to find this menu, refer to the instructions provided in the *No Security* configuration section.

2. Refer to the chapter *Configuring Device Level Databases* in order to select and configure the device level database.

USING MANAGE MODE

`seclevel`
Displays the current security level configuration data.

DEVICE LEVEL SECURITY BACKGROUND INFORMATION

Device level security is an authentication process between internetworking devices, in which authentication takes place automatically. Both bridges and routers support this form of security.Device level security is available to the network locally through the On-node Device Database or remotely through CSM or RADIUS Server.

Device level security is the default configuration. Through device level security, you have several options for validating remote devices and providing security for the network. The security options available are dependent on the remote device type and the line protocol in use.

The following tables summarize information needed for different device types:

Interface Type	*Associated Remote Device Type*	*Security Required?*
WAN	IP Host PPP	optional
WAN (Direct Host)	IP Host PPP	optional
WAN (RLAN)	HDLC Bridge PPP	REQUIRED
WAN (UnNumbered)	PPP	REQUIRED

Device Type	*Security Options*
PPP	CLID, CHAP, PAP
HDLC Bridge	CLID, MAC Address Security
IP Host	CLID, IP Host ID

Note: For further information regarding network interfaces and their corresponding configuration elements, refer to the network interface information refer to the network interface information in the *Configuring Basic IP Routing Options* chapter.

OVERVIEW OF DEVICE AUTHENTICATION PROCESS

When a remote device connects, the CyberSWITCH negotiates the required authentication. It then collects the information which is used to identify and authenticate the remote device. The system compares this collected information against information maintained in a device database. If the information collected from the remote device matches the information found in the database, the connection is valid and the device is allowed access to network resources. If the collected information does not match the information in the database, the connection is disconnected.

The device database can be maintained either locally on the CyberSWITCH itself, or on a server, central to the network. When an on-node device database is used, device information is configured either directly through the CFGEDIT configuration utility or through using Manage Mode commands.

It is also possible to configure and maintain device information on an off-node, central device database. This could be useful for networks with a large number of devices or several systems. Only one device database would need to be configured and maintained. The Remote Authentication Dial In User Service (RADIUS) and CSM are the off-node, central databases currently supported by the system. The RADIUS Server option is available for PPP / IP devices (with CHAP or PAP security), HDLC bridge devices, and RFC 1294 devices.

USER LEVEL SECURITY

CONFIGURING USER LEVEL SECURITY

USING CFGEDIT

1. Select *User Level Security* from the Security Level Menu. If you need guidance to find this menu, refer to the instructions provided in the *No Security* configuration section.

2. Refer to the chapter *Configuring User Level Databases* in order to select and configure the user level database.

USING MANAGE MODE

`seclevel`
Displays the current security level configuration data.

USER LEVEL SECURITY BACKGROUND INFORMATION

User level security is an authentication process between a specific user and a device. The authentication process is interactive; users connect to a terminal server and need to interact with it in order to communicate with other devices beyond the server. The CyberSWITCH supports user level security through the RADIUS, TACACS, or ACE server.

User level security supports the following devices:
- PPP devices
- HDLC bridges

The following sections provide information regarding authentication via SecurId cards, system requirements for user level security, and the authentication process with user level security.

AUTHENTICATION USING A SECURITY TOKEN CARD

The CyberSWITCH supports interactive, user level security through the TACACS or ACE server programmed for use with security token cards. Token cards are credit card-sized devices. These cards are widely used throughout the computer industry for authentication. This concept of authentication is now available to ISDN connections via the CyberSWITCH. The CyberSWITCH version of user level security supports a security token card called SecurID, provided by Security Dynamics.

The SecurID card works on a "passcode" concept, which consists of two factors:
- a known value (the device's password)
- a dynamically-generated value (from the SecurID card)

Note: For more information specific to the SecurID card, refer to the documentation provided by Security Dynamics Technologies Inc.

The user is prompted for the passcode value at login. The following description illustrates how the user level authentication process works:

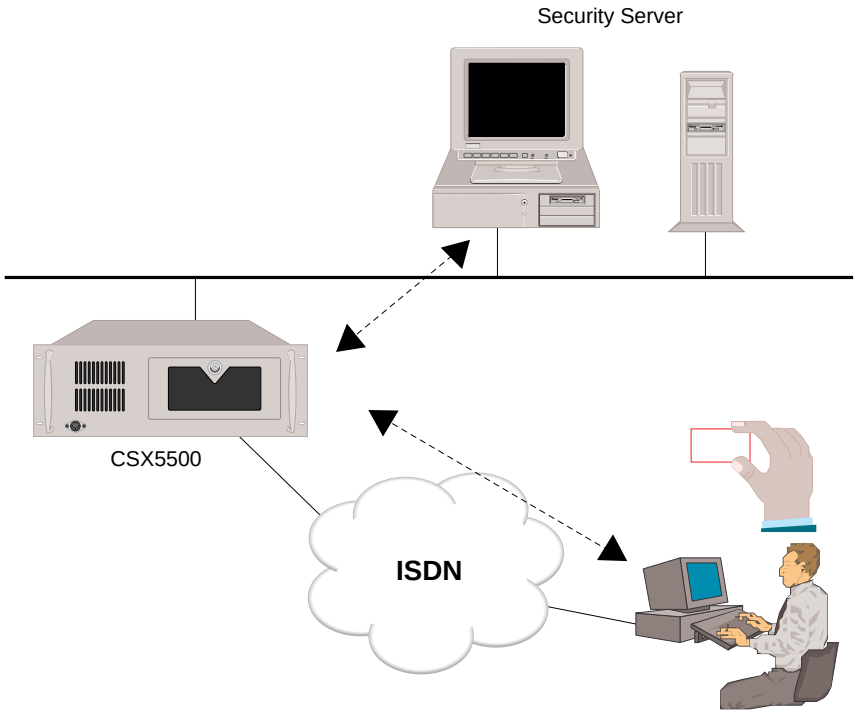
The CyberSWITCH provides user level security by having the remote user establish a Telnet connection to the system. While the remote user is being authenticated, a data filter is placed on the connection. This filter only allows the Telnet session traffic to flow over the connection between the user and the CyberSWITCH. During the Telnet session, the system collects user information (user Id, password and maybe dynamic password) and requests authentication from the configured server. Once the user is authenticated, the data filter is removed from that connection. All remote user data is now forwarded on the connection.

If the user fails to be authenticated, the connection is released. The user must establish a new connection and perform validation again.

If the ISDN connection is released by either the ISDN network or by the remote device, the system treats this as a new authentication session and starts the validation sequence over.

Note that when a user establishes the Telnet connection to the CyberSWITCH, the user needs to Telnet into a special TCP port configured for the type of authentication the user wishes to use. For example, to get validated through the TACACS authentication server, the user needs to Telnet into port 7000 (the default value for the TACACS port). Different port numbers are used for other types of authentication servers such as RADIUS or ACE.

The following picture shows the relationship between the security server, an end user, and the computer that prompts for the input. The security clients and the security server communicate with each other using some special protocol, such as TACACS.



SYSTEM REQUIREMENTS

When providing user level security for the CyberSWITCH, you must establish Remote User-to-LAN Connectivity (like terminal servers). You may not establish LAN-to-LAN Connectivity as routers usually do.

There are two different ways of establishing Remote User-to-LAN Connectivity:

- through IP Routing
- through Bridging

IP Routing connectivity refers to the connectivity between the CyberSWITCH and a remote device that can transfer IP datagrams over ISDN without MAC headers (such as an IP / PPP host device). Bridging connectivity refers to the connectivity between the CyberSWITCH and a remote user (computer) that is connected to the system through the ISDN bridge device. The remote computer and the ISDN bridge may be implemented as one device like the Bridge / PPP device or the WaveRunner in the Combinet emulation mode.

You must configure your CyberSWITCH keeping these stipulations in mind. Once your system is properly configured, and your authentication server is properly configured, you may access user level security by performing the following:

- making the appropriate Telnet connection
- responding correctly to the LOGIN prompts

AUTHENTICATION PROCESS WITH USER LEVEL SECURITY

Making a Telnet Connection

In order to access user level security, you must first establish a Telnet connection to the CyberSWITCH. Depending upon your application, the prompts or procedures may vary; however, the information you need to provide is as follows:

- host name: provide the IP address of the CyberSWITCH
- port #: provide the port number of the authentication server that is connected to the system
- emulation: VT100

Note that the system must be connected to the authentication server on the local LAN. Use the default value of the port number for the authentication server (RADIUS 7001, TACACS 7000, ACE 7003), unless you have changed this value in CFGEDIT. The emulation default is VT100. No change is required.

Once the Telnet connection is established, you will be prompted with a login screen.

Responding to LOGIN Prompts

The login display may vary, depending upon your database location, and the prompt order you have configured. Responses to prompts may vary, depending upon whether or not you have a security token card, and the type of security token card you have. The ACE and TACACS servers support the SecurID card; the RADIUS server does not.

If using the RADIUS server for user level authentication, enter your user Id and password onto your remote machine.

If using the ACE or TACACS server for user level authentication, procedure depends upon type of security token card.

With the SecurID PINPAD card, you enter your password onto the SecurID card, which in turn generates a dynamic password or passcode.

With the SecurID non-PINPAD card, you enter your password onto your remote machine. You then check your SecurID card for its current dynamic password or passcode.

The difference in card function is that the PINPAD card generates a dynamic password or passcode based upon your password entry; the non-PINPAD card generates a new dynamic password based upon an elapsed period of time.

Refer to the section below that summarizes the login procedure required for the type of server you are using.

RADIUS:

does not use security token card

1. Enter login Id.
2. Enter password.

TACACS:

with PINPAD SecureID Card

1. Enter login Id (remote machine).
2. Enter password onto SecurID card, which generates a dynamic password.
3. Enter dynamic password onto remote machine's password prompt.
4. Press <RET> key when prompted for dynamic password.

with non-PINPAD SecureID Card

1. Enter login Id (remote machine).
2. Enter password (remote machine).
3. When prompted for a dynamic password, enter the dynamic password that is currently displayed on your SecurID card onto your remote machine.

ACE:

with PINPAD SecureID Card

1. Enter login Id (remote machine).
2. You will be prompted for a passcode. To generate a passcode, enter your PIN onto the SecurID card. The SecurID card will then generate a passcode.
3. Enter the SecureID passcode at the remote machine prompt.

with non-PINPAD SecureID Card

1. Enter login Id (remote machine).
2. At the passcode prompt, enter your 4-digit PIN followed by the 6-digit dynamic password on your SecurID card. (This makes up your passcode).

Note: Password (RADIUS) is an encrypted password value, 1 to 12 ASCII characters in length. Password or PIN (TACACS or ACE) is a personal identification number, 1 to 4 numeric characters in length. Dynamic password or passcode is the 6-digit numeric value generated by the SecurID card.

DEVICE AND USER LEVEL SECURITY

CONFIGURING DEVICE AND USER LEVEL SECURITY

USING CFGEDIT

1. Select *Device and User Level Security* from the Security Level Menu. If you need guidance to find this menu, refer to the instructions provided in the *No Security* configuration section.

2. Refer to the chapters *Configuring Device Level Databases* and *Configuring User Level Databases* in order to select and configure the device level database and the user level database.

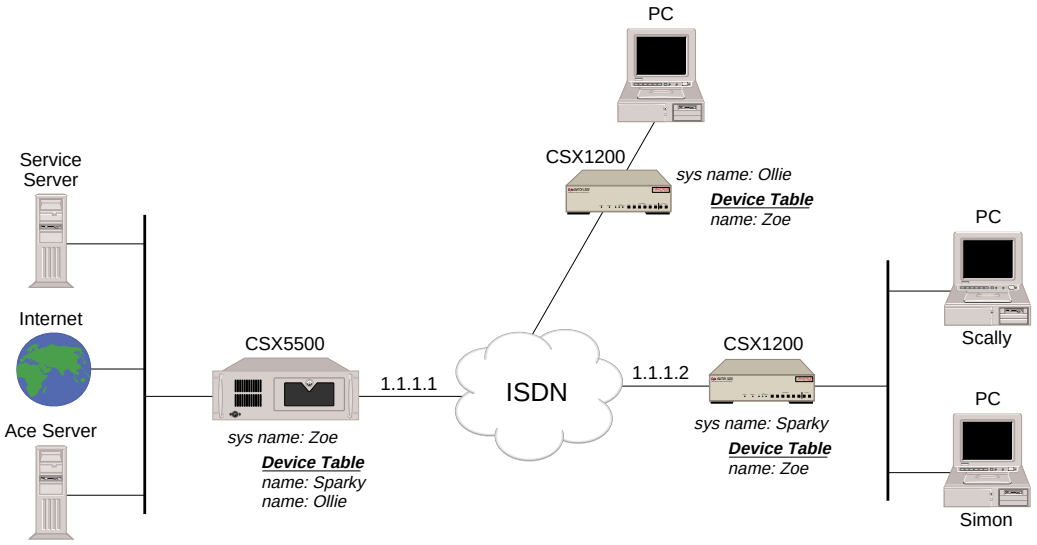
USING MANAGE MODE

seclevel

Displays the current security level configuration data.

DEVICE AND USER LEVEL BACKGROUND INFORMATION

Multi-level security (device and user level) provides you with increased security options for your network. This feature supports device level security for all remote devices. User-level authentication can be performed on top of device level authentication for IP, IPX, AppleTalk and bridge users. Only users configured for user level authentication will be required to do so. Refer to the following illustration of a sample IP network configured for multilevel security.



The network security level has been configured for both device level and user level security. Certain remote devices, such as Ollie, are able to dial-in and are only authenticated at the device level. However, remote devices, such as Sparky, are configured in the device level database to be authenticated at the user level as well as at the device level.

For example, Scally is using the PC on the LAN attached to Sparky, a CSX1200. Scally needs to download some files off of the Service Server, which is on the LAN connecting to Zoe, a CSX5500. Upon initiation of Scally's call, device level authentication begins. Zoe checks its on-node device database to see if Sparky is a valid device, and whether its IP address and password are also valid. If valid, Zoe allows the connection, however a data filter is placed on the connection. This filter only allows Telnet session traffic to flow over the connection between Zoe and Sparky. User level authentication begins when Scally telnets to the IP address 1.1.1.1, port 7003, which is the port assigned to the ACE server. Zoe sends the user level login prompt to Scally's PC. Once Scally completes the login and password information, Zoe relays this data to the ACE Server. If Scally is a valid user in the ACE database and provides the correct login and password, Zoe removes the restrictive filter so he may access the Service Server, or any other system on that LAN. Now that Scally has been properly authenticated, any users on his LAN may access the systems attached to Zoe. For example, while Scally is downloading files, Simon could boot up his PC and access the Internet without going through the authentication process.

CONFIGURING SYSTEM OPTIONS AND INFORMATION

OVERVIEW

System options include security options for remote devices. The security required for the authentication of each device will depend on the information you have entered for that device.

System information includes a system name, system password, and a system secret. These values are required only if there are remote devices on the network that require this information for system validation.

The system software allows you to achieve secure administrative sessions, along with flexible control. Administration security enhancements include selecting a database server for administration sessions and specifying an inactivity time-out. In addition, you can restrict Telnet access by setting the number of possible administrative Telnet sessions, and you can configure another Telnet port to accept an emergency Telnet Server session.

SYSTEM OPTIONS

CONFIGURING SYSTEM OPTIONS

USING CFGEDIT

1. Select *Security* from the main menu.

2. Select option (2), *System Options and Information* from the Security Menu. The following screen be displayed:

```
System Options and Information Menu:

   1) System Options
   2) System Information
   3) Administrative Session

Select function from above or <RET> for previous menu: 1
```

3. Select (1) *System Options*. The following screen will be displayed:

```
System Options Menu:


PPP Link:
   1) PAP Password Security              ENABLED
   2) CHAP Challenge Security            ENABLED


HDLC Bridge Link:
   3) Bridge MAC Address Security        ENABLED


IP Host (RFC 1294) Link:
   4) IP Host Id Security                ENABLED


ISDN:
   5) Calling Line Id Security           ENABLED

Id of the Option to change or <RET> for previous menu:
```

Note: It is not necessary to disable a security option, even if you are not using the option. The security required for the authentication of each device will depend on the information you have entered for that device. If, for some reason, you wish to disable an option, select the Id of the option and press <RET>.

SYSTEM OPTIONS CONFIGURATION ELEMENTS

CALLING LINE ID SECURITY

Validates the Calling Line information received when an ISDN connection is made. The system will compare the incoming Calling Line Id with the value configured (if any) in the Device List. If the numbers are identical the connection will be established. Otherwise, the system will reject the incoming call.

When the Calling Line Id security is enabled, entering a Calling Line Id for each remote device is optional. When two remote devices share the same line (a single point-multipoint ISDN line), they can also configure the same Calling Line Ids if they both also have some other type of authentication configured (for example, PAP, CHAP, or Bridge MAC Address Authentication).

The following table illustrates the dependencies between other authentication methods and the Calling Line Id authentication:

PAP Authentication	*CHAP Authentication*	*Bridge MAC Address Authentication*	*Calling Line Id Authentication*
Yes	No	No	Optional Duplicates allowed for these Devices.
No	Yes	No	Optional Duplicates allowed for these Devices.
No	No	Yes	Optional Duplicates allowed for these Devices.
No	No	No	Required Duplicates not allowed.

Note: If a system is brought on line with a device that has a required Calling Line Id that is a duplicate of another device's Calling Line Id, and no other type of authentication is used, a warning message is logged at initialization. Every attempt to connect the device thereafter will result in an error message being logged and the call being rejected.

PAP PASSWORD SECURITY

PAP Security provides a method for the Device to identify itself to the system using a 2-way handshake. If PAP Password Security is enabled, and a PAP Password has been configured for the Device, the following holds true:

- After the initial connection is made, the Device Name and Password are repeatedly sent by the remote device to the system. The system will look up the received Device Name in the Device List.
- If the Device Name is not found, the call is disconnected.
- If the Device Name is found the system will validate the password.
- If the password does not match, the call will be disconnected.
- If PAP Password Security is enabled, and a PAP Password has not been configured for the Device, Password validation is not performed.

CHAP CHALLENGE SECURITY

An authentication phase between the remote device and the system begins with sending a CHAP challenge request to the remote device. The CHAP request contains a string of bytes known as the challenge value, which is changed on each challenge. Using the hash algorithm associated with CHAP, the remote device transforms the challenge value plus its secret into a response value. The remote device sends this output of the hash function, along with its symbolic name, to the system in a CHAP response.

Within the Device Table entry for each remote device which will be authenticated via CHAP, the system maintains the remote device's secret. The name in the remote device's CHAP response is used to locate the Device Table entry, and consequently the secret used by the remote device. Using the same hash function, the system computes the expected response value for the challenge with that secret. If this matches the response value sent by the remote device, a successful authentication has occurred. The system can optionally be configured to repeat the CHAP challenge process periodically throughout the life of the connection. An invalid response to a CHAP challenge at any time is deemed a security violation, which causes a switched link to be released.

The above process applies to the system's authentication of the remote device. It is also possible that the remote device may wish to authenticate the system itself, a desire that is also negotiated during the LCP initialization of the link. Enabling CHAP via configuration also permits the system to agree to be authenticated via CHAP during LCP negotiation. In the same manner that each remote device has a name and secret, the system itself is configured with a system-wide name and secret that are used to respond to CHAP challenges.

Note: When both CHAP and PAP are enabled, the system will request the CHAP protocol first. If the remote device agrees to CHAP, then the secret that is configured for the device must match the one that the remote device uses. If the remote device agrees to PAP then the passwords must match. If only one of either PAP or CHAP is enabled, the system will insist on that protocol only. If the remote device does not support the enabled protocol, the device will not be allowed

BRIDGE MAC ADDRESS SECURITY

If bridging is enabled, you have the option of enabling Bridge Ethernet Address Security. Bridge MAC Address Security may also be enabled if IP routing through a Virtual WAN interface is enabled. This security option allows you to configure specific Bridge Ethernet Addresses and an optional password on a per device basis. When Bridge Ethernet Address security is enabled, the System will look up the received Ethernet address in the Device List. If the address is not found, the call is disconnected. If the address is found and the corresponding device entry is configured with a password, the System will validate the password. If the password is not valid, the call will be disconnected.

IP HOST ID SECURITY

To enable IP Host Id Security, you must first enable IP routing. IP Host Id Security provides added security through device validation. At connection establishment time, the Device sends an unencrypted IP Host identifier over the WAN to the System. The System looks up the Device based on the received IP Host identifier. If the identifier is found in the Device List, the call is accepted. Otherwise the call is disconnected.

SYSTEM OPTIONS BACKGROUND INFORMATION

When a remote device connects, the CyberSWITCH negotiates the required authentication. In order for the remote device to be properly authenticated, the CyberSWITCH must have the appropriate authentication enabled. If the CyberSWITCH does not have the authentication required by the remote device enabled, the remote device will not be authenticated and the call will be disconnected.

The possible security options that can be enabled include:

- Calling Line Id
- IP Host Id
- Bridge Ethernet Address
- PAP
- CHAP

The following table summarizes the identifying and authenticating information used by each remote device type to connect to the system:

Device Type	*Identifier*	*Authenticator*
HDLC Bridge (MAC Layer Bridge)	Bridge Ethernet Address or Calling Line Id	Bridge Ethernet Address Optional: Password Optional: Calling Line Id
IP Host (with RFC 1294 encapsulation)	IP Host Id	IP Host Id Optional: Calling Line Id
PPP	Device Name	CHAP Secret or PAP Password Optional: Calling Line Id

SYSTEM INFORMATION

CONFIGURING SYSTEM INFORMATION

USING CFGEDIT

1. Select option (2), *System Information* from the System Options and Information menu. If you need guidance to find this menu, refer to the instructions provided in the *System Options* configuration section. The following screen will be displayed:

```
System Information Menu:

   1) System Name         is "ralph"
   2) System Password     is "ralph"
   3) System Secret       is "ralph"

Select function from above or <RET> for previous menu: 1
```

2. Select the option you wish to configure and press <RET>. Follow the onscreen instructions to configure the option you select. These values are required only if there are remote devices on the network that require this information for system validation.

SYSTEM INFORMATION CONFIGURATION ELEMENTS

SYSTEM NAME

The System Name is a user-defined name for the CyberSWITCH. This name is preconfigured, but may be changed. It is from 1 to 17 ASCII characters in length. The System Name is only used if there are remote devices on the network that require this information for system validation. This name is passed in the name field during PAP negotiation.

SYSTEM PASSWORD
The System Password is a user-defined password that is only required if there are remote devices on the network that require this information for system validation. This is passed in the password field during PAP negotiation. This password can be from 1 to 17 ASCII characters in length.

SYSTEM SECRET
The System Secret is a user-defined shared secret that only needs to be configured if there are remote devices on the network that require this information for system validation. The same System Secret must also be configured on the remote device. The Shared System Secret is used during CHAP negotiation. The System Secret can be from 1 to 17 ASCII characters in length.

SYSTEM INFORMATION BACKGROUND INFORMATION

The System Information is only required if remote devices on the network require this information for system validation. The System Name is passed during both PAP and CHAP negotiation. The System Password is passed during PAP negotiation. The System Secret is the CHAP Secret used during CHAP negotiation.

ADMINISTRATIVE SESSION

CONFIGURING ADMINISTRATIVE SESSIONS

USING CFGEDIT

1. Select *Security* from the main menu.

2. Select *Administrative Session* from the Security Menu. The following menu is then displayed:

```
Administrative Session Menu:

   1)  Authentication Database Location    is On-node
   2)  Session Inactivity Timeout          is DISABLED
   3)  Number of Admin Telnet Sessions     is 3
   4)  Telnet Server TCP Port Number       is 23
   5)  Emergency Telnet Server Port Number is 9000

Select function from above or <RET> for previous menu: 1
```

3. Select option (1) to configure the authentication database location for the administration sessions. The following menu will be displayed:

```
Administrative Session Database Location Menu:

Database Location
   1) On-node
   2) CSM
   3) RADIUS
   4) TACACS
   5) ACE

Current Database Location is "On-node".

Select function from above or <RET> for previous menu:
```

4. You may specify an authentication database location for administrative sessions that is different from the user authentication database location.

   Note: If you select RADIUS, TACACS, or ACE, you must be sure that the selected server is active before you initiate an administrative session.

5. From the Administrative Session menu select (2) *Session Inactivity Timeout*. The following prompt is displayed:

```
Enter the Session Inactivity Timeout value in minutes.
Use "0" to disable the Session Inactivity Timeout [default = disabled]?
```

6. Follow the onscreen instructions to set the session inactivity timeout session.

7. From the Administrative Session menu, select (3) *Number of Admin Telnet Sessions.* The following prompt is displayed:

```
Enter the number of Telnet allowed for administrative sessions.
Use "0" to disable the Telnet Server [default = 3]? 1
```

8. Follow the onscreen instructions to configure the number of administrative Telnet sessions you wish to allow. Up to three sessions are possible.

   Note: To have any Telnet sessions, you must first enable IP.

9. To change the value of the port number, select (4) *Telnet Server TCP Port Number* from the from the Administrative Session menu.

10. Follow the onscreen instructions for entering the port number.

11. Select option (5) *Emergency Telnet Server Port Number* from the Administrative Session menu.

12. Follow the onscreen prompts to configure the port number.

USING MANAGE MODE

`admlogin`
Displays the current administration session configuration.

`admlogin change`
Displays the Administration Session Configuration Menu screen, allowing you to change the authentication database location. Refer to *Using CFGEDIT* for configuration instructions.

ADMINISTRATIVE SESSION CONFIGURATION ELEMENTS

DATABASE LOCATION
The authentication database location for administration sessions. This database location may be different from the user authentication database. The default database location is the on-node device database.

TIMEOUT VALUE
Allows you to terminate login sessions after the configured “time-out value” length in time. If “0” is entered, the value will be disabled. The time-out will be enabled by entering a number greater than 0. The range is from 0 to 1,440 minutes.

NUMBER OF SESSIONS
This value disables, or limits the number of Telnet administrative sessions allowed. The default value and the maximum value is 3. If 0 is entered, the Telnet server will be disabled.

TELNET SERVER TCP PORT NUMBER
The port number of the Telnet Server TCP Port. The default value is 23.

EMERGENCY TELNET SERVER TCP PORT NUMBER
The port number for emergency Telnet sessions. The default for this emergency port is 9000.

ADMINISTRATIVE SESSION BACKGROUND INFORMATION

ALTERNATIVE DATABASE LOCATION BACKGROUND INFORMATION

In addition to using the local password file to validate a remote device who wishes to login to the CyberSWITCH, you may also choose to use an off-node database server such as TACACS or ACE. Using the off-node server allows you to share the password file on the database server for multiple systems. It may also provide more secure access to the CyberSWITCH: some of the platforms are PCs, and files on those platforms could be changed, while the database server can be physically more secure.

As an alternative to the local password file, the user can now use security token cards along with the TACACS or the ACE server, which provide the use of dynamic, one-time password capability.

SESSION INACTIVITY BACKGROUND INFORMATION

This option may be set to terminate login sessions after a configured inactivity timeout period. Since there are only a limited number of sessions available, this avoids the problem of administrator lockout because a user forgets to logout from the system.

NUMBER OF ADMINISTRATIVE TELNET SESSIONS BACKGROUND INFORMATION

Whenever IP routing is enabled, three Telnet sessions are available for system administration. Telnet access is a very useful method to manage the CyberSWITCH remotely, but there may be a case where it is desirable to disable the Telnet access for security reasons. With this configuration option, Telnet access to the system can be disabled, or the number of Telnet sessions can be limited to less than 3.

TELNET SERVER TCP PORT NUMBER BACKGROUND INFORMATION

TCP stands for Transmission Control Protocol, which uses IP to deliver its packets. The default value for this port is 23. However, if you choose to use a different port number, you may adjust this value through CFGEDIT. The Client must be aware of the port number you have configured.

EMERGENCY TELNET SERVER PORT NUMBER BACKGROUND INFORMATION

There are some Telnet client programs that do not clear Telnet connections when terminating Telnet sessions. Since they do not clear the Telnet connections, those connections stay alive and soon all Telnet sessions are used up. Once this happens, no more Telnet sessions can be established until the inactivity timer of one of the sessions expires.

However, if the idle timer of the administrative session is disabled, you may need to reboot the CyberSWITCH. To avoid this, a special Telnet server that uses a particular TCP port is provided. If you Telnet into this special server (the Emergency Telnet Server) you will be placed into a session which prompts you for an action on each of the existing Telnet sessions.

The emergency Telnet session allows you to terminate Telnet sessions only when all Telnet sessions are used up. An emergency Telnet server is available to clean up dead Telnet sessions. This Telnet server needs a unique port number in order to function.

The following example screen illustrates a successful emergency Telnet session:

```
Emergency Telnet session active
Enter password(s) for 'ADMIN' user.
Enter password: ******

 Login-Id Sess-Id Date/Time    Idle (sec) Command Type (From)
 -------- ------- ------------ ---------- -------- ------------------------
 ADMIN    257     May 20 12:34 800        MANAGE   Telnet (199.120.211.70)

Do you wish to terminate this session (Y or N) [default = Y]? <RET>

 Login-Id Sess-Id Date/Time    Idle (sec) Command Type (From)
 -------- ------- ------------ ---------- -------- ---------------
 ADMIN    511     May 20 12:30 1025       SHELL    199.120.211.71

Do you wish to terminate this session (Y or N) [default = Y]? <RET>

 Login-Id Sess-Id Date/Time    Idle (sec) Command Type (From)
 -------- ------- ------------ ---------- -------- ---------------
 ADMIN    734     May 20 12:35 740        LOGIN    199.120.211.69

Do you wish to terminate this session (Y or N) [default = Y]? <RET>
```

The following screen illustrates a situation where Telnet sessions are still available. The Emergency Telnet session then simply informs you that you can not terminate Telnet sessions under these circumstances (no emergency exists).

```
Emergency Telnet session active
Enter password(s) for 'ADMIN' user.
Enter password: ******

There are Telnet connections available for administrative sessions.
Please use an administrative session to terminate abandoned sessions.
```

CONFIGURING DEVICE LEVEL DATABASES

OVERVIEW

Device level security is an authentication process between internetworking devices, in which authentication takes place automatically. Both bridges and routers support this form of security.Device level security is available to the network locally through the On-node Device Database or remotely through the Connection Services Manager (CSM) or RADIUS Server.

This chapter provides information for enabling and configuring the on-node device database, and enabling an off-node database location. If an off-node database location is specified, refer to the chapter *Configuring Off-node Server Information* for configuration instructions.

ON-NODE DEVICE DATABASE

CONFIGURING AN ON-NODE DEVICE DATABASE

Before configuring an on-node device database, you must first configure network interfaces. For further information regarding network interfaces and their corresponding configuration elements, refer to:

- *IP Network Interfaces* for IP Routing
- *IPX Network Interfaces* for IPX
- *AppleTalk Port Information* for AppleTalk

USING CFGEDIT

1. To begin the configuration of an on-node database or any of the Security Database options, start at the main menu and progress through the screens as shown below:

```
Main Menu:

   1) Physical Resources
   2) Options
   3) Security
   4) Save Changes

Select function from above or <RET> to exit: 3
```

```
Security Menu:

   1) Security Level
   2) System Options and Information
   3) Device Level Databases
   4) User Level Databases (Enable/Disable)
   5) Off-node Server Information
   6) Network Login Information

Select function from above or <RET> for previous menu: 3
```

```
Device Level Databases Menu:

   1) On-node Device Database (Enable/Disable)
   2) On-node Device Entries
   3) Off-node Device Location

Select function from above or <RET> for previous menu: 1
```

2. Select option (1) *On-node Device Database* from the Device level Databases menu. The following screen will be displayed. Follow the on-screen instructions to enable the on-node database device:

```
On-node Device Database (Enable/Disable) Menu:

   1) On-node Device Database is currently: ENABLED

Select function from above or <RET> for previous menu: 1
```

ON-NODE DEVICE ENTRIES

CONFIGURING ON-NODE DEVICE ENTRIES

1. Select *On-node Device Entries* from the Device Level Databases menu.

2. The Current Device Table screen will be displayed. Follow the onscreen instructions to add a device:

```
Current Device Table (Sorted by Device Name in Ascending ASCII Order)

Id     Device Name
---------------------------

There are currently no Devices configured.

   1) Add a Device or press <RET> for previous menu: 1
```

3. Enter the device name. The example screen below shows device DAN being added:

```
Device Name? DAN
```

4. The Device Table menu will then be displayed similar to the example screen shown below:

```
Device Table Menu: (Device = "DAN")

   1)  ISDN
   2)  Frame Relay
   3)  X.25
   4)  Digital Modem
   5)  Authentication
   6)  IP
   7)  IPX
   8)  AppleTalk
   9)  Bridge
   10) Compression
   11) Encryption

Select function from above or <RET> for previous menu: 1
```

   We suggest that you first enter the information pertaining to the device's access type(s). Access types include: ISDN (which also includes configuration elements for devices connecting over dedicated links), Frame Relay, X.25, and Digital Modem (see above menu). Most devices use an ISDN access, in which case you would complete the information under *ISDN*. Note that it is possible for a device to primarily use Frame Relay or X.25, with ISDN as a backup access. In this case, you would enter *ISDN* information in addition to *Frame Relay* or *X.25 information*. Digital Modem accesses require no ISDN access configuration; simply complete the information under *Digital Modem*.

   Refer to the section(s) below that pertain to the device's access type. Then continue with the rest of the device configuration.

5. For ISDN (and dedicated) devices, begin by selecting *ISDN* from the Device Table Menu. The following menu will be displayed with the shown preconfigured default values:

```
Device ISDN Menu: (device = "DAN")

   1) ISDN Line Protocol.       "PPP (Point to Point Protocol)"
   2) Base Data Rate.           "64000 bps"
   3) Initial Data Rate.        "64000 bps"
   4) Maximum Data Rate.        "128000 bps"
   5) Dial Out Phone Number(s). ""
   6) Subaddress.               ""
   7) Profile Name.             "Default_Profile"
   8) H0 Call Support           DISABLED

Select function from above or <RET> for previous menu: 1
```

   a. If you will not be using the default of *PPP* as your line protocol, select (1), ISDN Line Protocol and select the type you will be using.
   b. Check to see if the default base data rate, initial data rate, and maximum data rate are acceptable. If not, change the default values through the above menu (selections 2, 3, and 4). From the same menu, you will also need to configure the first dial-out number (if you want dial-out capabilities to this device).
   c. The Profile Name pertains to the Bandwidth Reservation feature. The Device Profile entry identifies which line or lines are reserved for a particular profile.
   d. H0 Call Support can be enabled for devices who need more bandwidth to accomplish large file transfers or video conferencing.

6. For Frame Relay devices:

   Note: You must first configure the Frame Relay Access. Instructions for configuring the access is found in the *Frame Relay Accesses* section of the *Configuring Alternate Accesses* chapter.

   Begin by selecting *Frame Relay* from the Device Table Menu. A screen similar to the following is displayed:

```
Device Frame Relay Menu: (Device = "DAN")

                         Access Name           DLCI    Protocol
    1) PVC Information   DANACCESS             16      PPP

You cannot change this information from within this menu.

Press any key to continue
```

   This screen will reflect your previously-configured *access information* for a permanent virtual circuit associated with the device. This information is not configurable in this location.

   Notes: If you receive the following message, ensure that the PVC Name matches the device name.

```
No pvc configured for Device "DAN"
```

   In order to associate a device to a specific PVC, you must also provide authentication information (see step 9).

7. For X.25 devices:

   Note: You must first configure the X.25 Access. Instructions for configuring the access is found in the *X.25 Accesses* section of the *Configuring Alternate Accesses* chapter.

   Begin by selecting *X.25* from the Device Table Menu. If the X.25 access is configured for both PVCs and SVCs, select the type of virtual circuit for the device:

```
Select the type of the Virtual Circuit
   1) Permanent Virtual Circuit (PVC)
   2) Switched Virtual Circuit (SVC)   [default 2]:
```

If you select PVC, the list of available PVCs are displayed. The LCN of the selected PVC and the X.25 Access Name are stored in the Device Table to bind the device to a particular virtual circuit configuration:

```
Select the type of the Virtual Circuit
   1) Permanent Virtual Circuit (PVC)
   2) Switched Virtual Circuit (SVC)   [default 2]: 1

Current Permanent Virtual Circuits defined for X.25 Access #1, 'VMAX25':

 id Type LCN   Protocol
 -- ---- ---- --------
 1   PVC   1     RFC877
 2   PVC   2     RFC877

Id of Virtual Circuit to associate with device "vma",
 or <RET> to cancel?   1
```

If you select SVC, you must enter the X.121 address of the remote DTE. You need the remote DTE address to make the X.25 call to the proper remote device.

```
Select the type of the Virtual Circuit
   1) Permanent Virtual Circuit (PVC)
   2) Switched Virtual Circuit (SVC)   [default 2]: 2

Enter the X.121 Address of the Remote DTE
or press <RET> to cancel? 9987654321
```

8. For Digital Modem devices:

   Begin by selecting *Digital Modem* from the Device Table Menu. The following menu will then be displayed:

```
Device MODEM Menu: (device = "DAN")

   1) Line Protocol            "PPP (Point to Point Protocol)"
   2) Baud Rate                "Auto"
   3) Bearer Capabilities      "Speech"
   4) Dial Out Phone Number(s) ""

Select function from above or <RET> for previous menu:
```

   a. No change is necessary for Line Protocol. At this time, only PPP is available.
   b. No change is necessary for Baud Rate. At this time, only Auto is available.
   c. Select the line's bearer capabilities.
   d. Enter the phone number for this device.

   Note: For detailed instructions on setting up your CyberSWITCH for Digital Modem usage, refer to *Configuring Other Advanced Options*.

9. Enter the authentication information needed. To begin entering the information, select *Authentication* from the Device Table Menu. The following menu will then be displayed:

```
Device Authentication Menu: (device = "DAN")

PPP:
   1) PAP Password                  ""
   2) CHAP Secret                   ""
   3) Outbound Authentication       ENABLED
   4) User Level Authentication     DISABLED


IP Host (RFC 1294):
   5) IP Host Id                    ""


HDLC Bridge:
   6) Bridge Ethernet Address       ""
   7) Bridge Password               ""


ISDN:
   8) Calling Line Id(s)            ""

Select function from above or <RET> for previous menu:
```

Provide the necessary device authentication information for your selected Line Protocol. (Refer to *On-node Device Database Security Requirements* for details). For example, for a PPP device, specify a CHAP secret. Or, for an HDLC device, enter a Bridge Ethernet Address.

For PPP, the ability to enable / disable outbound authentication (selection 3) is available. However, it is generally not necessary to enable outbound authentications on a point-to-point line. If the device is associated with a frame relay virtual circuit, and the PVC name is different than the device name, then outbound authentication is required.

In addition, if you want to add user-level security to IP, AppleTalk and bridge devices, you may also enable User Level Authentication. This requires the user that initiates a connection between the remote device and the CyberSWITCH to be authenticated at the user level as well. Refer to *Device and User Level Security* for details.

Note: Do not enable User Level Authentication for terminal server devices which connect through the digital modem.

10. To enter any needed IP information for your device, select *IP* from the Device Table Menu. The following screen will be displayed:

```
Device IP Menu: (device = "DAN")
   1) IP Address                            NONE
   2) IP Routing                            ENABLED
   3) Make calls for IP data                ENABLED
   4) IP Input Filter                       NONE
   5) IP Output Filter                      NONE

Select function from above or <RET> for previous menu:
```

If your device requires an IP address, enter it now. Options are:

- *none* for Direct Host or WAN links that plan to use dynamic address allocation
- *0.0.0.0* for unnumbered WAN links
- *IP address #* for traditional numbered WAN links

Enable or disable IP routing for this device.

If you want dial-out capabilities to this device, enable *Make calls for IP data.*

If you want to apply a predefined forwarding filter to this device, specify the filter name here. Refer to *Forwarding Filters* for more information.

11. To enter any needed IPX information for your device, select *IPX* from the Device Table Menu. The following screen will be displayed:

```
Device IPX Menu: (device = "DAN")

   1) IPX Routing             DISABLED
   2) Make calls for IPX data DISABLED
   3) IPXWAN Protocol         DISABLED
   4) IPX Routing Protocol    NONE
   5) IPX External WAN NetNum NONE
   6) Spoofing Options

Select function from above or <RET> for previous menu:
```

   a. Enable or disable IPX routing.
   b. If you enable IPX routing and want dial-out capabilities to this device, enable the *Make Calls* feature.
   c. If you enable IPX routing, you may enable or disable *IPXWAN protocol*.
   d. If you enable IPX routing, select *IPX Routing Protocol*. Select a routing protocol of *none, RIP/SAP*, or *Triggered RIP/SAP*. When you select *Triggered RIP/SAP*, you will need to identify the WAN peer type as either *active* or *passive.*
   e. If you plan to use IPX over Frame Relay, and if you are also using a CSX200 or CSX400 on the other side of the Frame Relay connection, select *IPX External WAN Net Num*. Provide a unique number that you will also reflect on the CSX200 or CSX400 platform.
   f. You may also select *Spoofing Options*. Make changes to default spoofing setup, if desired.

   Refer to *IPX Information for Devices* and *Configuration Elements* for more information.

12. To enter any needed AppleTalk information for your device, select *AppleTalk* from the Device Table Menu. The following screen will be displayed:

```
Device AppleTalk Menu: (device = “DAN”)

   1) AppleTalk Routing               DISABLED
   2) AppleTalk Address               None
   3) Make calls for AppleTalk data   DISABLED
   4) AppleTalk Routing Protocol      None

Select function from above or <RET> for previous menu: 1
```

   a. *Press 1* at the above menu, then follow the on-screen instructions to enable AppleTalk routing for the device.

b. *Press 2* at the above menu to enter the device's AppleTalk address. If the device is over an unnumbered link, enter 0.0. If the device is over a MAC dial-in port, you may either enter an address, or leave the value at "none".
c. *Press 3* at the above menu, then follow the on-screen instructions to configure whether or not dial out to this device is allowed for this device.
d. *Press 4* at the above menu to specify an AppleTalk routing protocol the system should use with this device. The options are *None* or *RTMP*. Currently RTMP is only supported for devices who will be dialing into the CyberSWITCH via a MAC dial-in port.

Note: If you are configuring a device for AppleTalk Remote LAN, leave the above AppleTalk information at the default values (*DISABLED, None, DISABLED, None*).

Refer to *AppleTalk Configuration Elements* for more information.

13. To enter any needed bridge information for this device, select *Bridge* from the Device Table Menu. The following screen will be displayed:

```
Device Bridging: (device = "DAN")

   1) IP (Sub)Network number        NONE
   2) Bridging                      ENABLED
   3) Make Calls for Bridge data    NONE
   4) IPX Remote LAN Network Number NONE
   5) IPX Spoofing Options
   6) AppleTalk Network Number      NONE

Select function from above or <RET> for previous menu:
```

You may enable or disable bridging for this device. If this device is to use a Remote LAN interface or Remote LAN port, enable bridging. If you want dial out capabilities to this device, enable *Make calls for Bridge data.*

For IP Remote LAN networks, you must explicitly configure the IP (Sub)Network number.

For IPX Remote LAN networks, you may configure the IPX external network number, or you may leave the value at *NONE.* The IPX Spoofing Options for IPX Remote LAN devices are not available at this time. For additional information, please refer to the *Configuring IPX* chapter, *Remote LAN Devices*.

For AppleTalk Remote LAN networks, you may configure the AppleTalk network number/ range (used on the Remote LAN for this device), or you may leave the value at *NONE.*

14. To enable per-device compression information, select *Compression* from the Device Table Menu. The following menu will then be displayed:

```
Device Compression Menu: (device = "DAN")

   1) Compression                          ENABLED
   2) Starting PPP STAC-LZS Sequence Number   1

Select function from above or <RET> for previous menu:
```

a. If compression is not already enabled for this device, press 1 and follow the onscreen instructions to change the configuration to enabled.
b. If the remote device does not use 1 as the starting PPP STAC-LZS sequence number, press 2 to enter a new value for the starting sequence number.

USING MANAGE MODE COMMANDS

device

Displays the current Device Table. Included in this display is each device's ID and name. After the list has been displayed, you may enter a specific device Id to display detailed information for that device.

device add

Allows you to add a device entry to the Device Table. You will be prompted for the device name and device type. The rest of the information you will be prompted for will depend upon the device type you are configuring, and the security options that are enabled. Note that the device name is case sensitive. You are prompted for the device information similarly to the way you are prompted by CFGEDIT. Refer to the above section, *Using CFGEDIT* for instructions.

device change

Allows you to change information for a specific device entry. The current device table will be displayed. Enter the device Id or device name of the entry you wish to change. Note that the device name is case sensitive. Step through the configuration information displayed for the device, pressing <return> if you wish to keep the originally configured information, and entering new information where you want it changed. For a definition of the configuration elements, refer to the section, *On-node Device Database Configuration Elements*.

device delete

Allows you to delete a device entry for a specific device. The current device table will be displayed. Enter the device Id or device name of the device whose device entry you wish to delete. Note that the device name is case sensitive.

ON-NODE DEVICE DATABASE CONFIGURATION ELEMENTS

GENERAL CONFIGURATION ELEMENTS

DEVICE NAME

A 1 to 63-character, user-defined case-sensitive name that uniquely identifies the device to the system administrator. The name may contain any displayable ASCII character except the quote "" character. This name is displayed on the connection monitor window when the device connects to the system.

ISDN CONFIGURATION ELEMENTS

Note: These elements are configured for ISDN devices and devices over dedicated connections only.

ISDN LINE PROTOCOL

The available line protocols for ISDN access devices. Possible line protocols include:

- PPP
  Point-to-point protocol. Allows device to use TCP/IP. The default configuration value.
- HDLC Bridge
  HDLC encapsulated bridge frames are used to connect the system to remote bridges. It is the simplest line protocol, using a standard HDLC frame.

- IP Host (RFC 1294)
  RFC 1294 provides a simple security exchange at connection time, along with an encapsulation method for IP datagrams.

BASE DATA RATE

Only used for Dial-Out. This value represents the throughput on a B-channel or pre-ISDN link connecting the CyberSWITCH to a device. The data rate can be specified as either 56,000 or 64,000 bps. The default configuration for the base data rate is 64,000 bps. If 64,000-bps connections to the device are not possible, this value should be set at 56,000 bps.

INITIAL DATA RATE

Only used for Dial-Out. The initial data rate determines the bandwidth that will be attempted when opening the first wide area connection. This provides you with a mechanism to request that a group of parallel connections be made to a remote device rather than a single connection. This will allow data to begin to flow at greater rates without waiting for the Throughput Monitor to detect an overload condition. Calls will be made until an additional call would exceed the configured value. The value is configured as a number from 2,400 to 1,024,000. For example, if you have configured the Base Data Rate at 64 Kbps, and the Initial Data Rate at 256,000, the system would attempt to initially use four calls (connections) running in parallel (256,000 / 64,000 = 4). The default configuration for the Initial Data Rate is 64,000 bps.

MAXIMUM DATA RATE

The Maximum Data Rate is used to limit the total number of channels that can be committed to a single device (logical connection). This sets an upper boundary for line and capacity utilization. This upper boundary allows you to keep one remote device from crowding out other devices and using an unfair share of available resources. This parameter is enforced on inbound and outbound calls. The system will not accept or make a call when the added bandwidth will exceed the configured maximum. The value is configured as a number from 2,400 bps to 3,072,000 bps. You may configure any value in this range. For example, if you have configured the base data rate at 64,000 bps, and the maximum data rate at 512,000 bps, the system would use a maximum of eight calls (connections) running in parallel to open up bandwidth (512,000 / 64,000 = 8). The value need not be a multiple of the Base Data Rate. The default configuration for the maximum data rate is 128,000 bps.

Note: A condition may occur in which the number of connections has reached the point where the maximum data rate will be exceeded with the next additional connection, and yet the remote device may initiate another call to the system. This inbound call causes the maximum data rate to be exceeded and the system will drop a connection. If the remote device is auto-dialing, this flip-flop condition will continue until you manually correct the problem. To correct this problem, configure the Throughput Monitor information to be identical on the CyberSWITCH and the remote device, or disable Throughput Monitoring on one of the devices. The Internet Engineering Task Force (IETF) is working on a standard solution to this problem.

If you are using multiple connections running in parallel (i.e., to the same device), the maximum number of connections that can be aggregated is 32. For maximum performance, however, we recommend aggregating no more than eight connections at a time.

DIAL-OUT PHONE NUMBER(S)
This configuration element is required when the Dial-Out feature is used. The dial-out capability allows the CyberSWITCH to initiate connections to PPP or HDLC devices located at remote sites. A phone number must be defined for each remote device that will be dialed. This number includes any prefix digits, area codes, or extensions as required to dial the destination device. It is possible to specify eight phone numbers for the remote device.

The system dynamically controls the bandwidth in use between the system and other devices. This is accomplished by establishing and disconnecting up to 8 calls to a single remote site over the digital network. The system monitors the connections for utilization and will add and remove connections based on the device configurable parameters described above (Base Data Rate, Initial Data Rate, and Maximum Data Rate).

SUBADDRESS
The Subaddress is used by a CyberSWITCH when it attempts to make a connection to a remote device. A Subaddress allows the device to share a telephone number with other devices and yet still recognize calls destined for it.

PROFILE NAME
The device profile identifies which line or lines are reserved for a particular profile, which in turn are reserved for a particular device(s). The feature that uses this configuration element, *Bandwidth Reservation*, is described in detail, in the *Configuring Call Control* chapter.

H0 CALL SUPPORT
If enabled, provides support for ISDN H0 calls operating at 384 Kbps. This provides one full 384 Kbps channel through the ISDN network and reduces the overhead associated with aggregating multiple channels. It is also almost always less expensive than the equivalent six 64 Kbps calls.

Not all ISDN networks provide support for H0 calls. This is dependent upon the ISDN service provider as well as the switch manufacturer.

FRAME RELAY ACCESS CONFIGURATION ELEMENTS

Note: These elements are configured for Frame Relay devices only.

PVC CONFIGURED
Information of the already configured frame relay virtual circuit which will be used for connections to the remote device. Currently, only permanent virtual circuits (PVCs) are provided by frame relay. If this information appears in a device entry, frame relay will be used first for the connection (regardless of any backup ISDN information configured).

X.25 ACCESS CONFIGURATION ELEMENTS

Note: These elements are configured for X.25 devices only.

VIRTUAL CIRCUITS
Specify an already-configured virtual circuit (either PVC or SVC) to be used for connections to this remote device. (Any two communicating X.25 devices must have a virtual circuit association between them before they can exchange data.)

X.121 ADDRESS
If you choose an SVC for your virtual circuit, you must provide the X.121 address of the remote device you are currently adding to the Device Table. (The X.121 addresses for both local and remote devices are provided by your X.25 provider.)

DIGITAL MODEM CONFIGURATION ELEMENTS

Note: These elements are configured for digital modem devices only.

LINE PROTOCOL
The available line protocols for ISDN access devices. The only available selection at this time is *PPP*.

BAUD RATE
The baud rate at which data will be transmitted. The only selection at this time is *Auto*, which implies the CyberSWITCH and remote modem will negotiate the baud rate automatically.

BEARER CAPABILITIES
The information transfer capabilities that are used for digitized analog modem signals. Choices are: *Speech* or *3.1 kHz Audio.* The default value is *Speech*.

DIAL OUT PHONE NUMBER
The phone number the CyberSWITCH will use to call out to this device.

AUTHENTICATION CONFIGURATION ELEMENTS

PAP PASSWORD
This password is used by PPP line protocol for PAP authentication. This is an unencrypted password value (a string of 1 to 12 ASCII characters) used as a security check when PAP Password Security is enabled. (PAP is an authentication protocol defined in RFC 1334 as part of the PPP protocol suite.) At connection establishment time, the calling party sends an unencrypted device identifier and password combination over the WAN to the system. The system looks up the Device Name based on the received device identifier and validates the password for that device. If the password received matches the password configured for the identified device, the call is accepted. Otherwise, the call is disconnected.

This value is stored in the same location as the bridge password, so a change to one password affects the other.

CHAP SECRET
This field is used by PPP line protocol for CHAP authentication. This is a string of 1 to 17 ASCII characters that is used as a security check when CHAP Challenge Security is enabled. (CHAP is an authentication protocol defined in RFC 1334 as part of the PPP protocol suite.) CHAP is characterized by a highly secure challenge and response mechanism which is performed at connection setup, and which can optionally be repeated throughout the existence of the connection. A shared CHAP Secret is configured for the devices at both ends of the connection. Refer to *System Information,* system secret. As opposed to a password, a CHAP Secret is not sent across the link, and therefore is not susceptible to interception. Instead, a calculation is done on the packets transmitted between the two devices, and the results are compared to the shared CHAP Secret for validation. If the calculation's results do not match the expected results, the connection is terminated.

OUTBOUND AUTHENTICATION
This parameter allows you to enable or disable PPP outbound authentication procedures. When PPP outbound authentication is enabled, PPP (CHAP or PAP) authentication is required at both ends of the connection. When PPP outbound authentication is disabled, the CyberSWITCH does not authenticate the remote device when dialing out. If enabled, the CyberSWITCH will authenticate the remote device. Outbound authentication is required if a PPP device is associated with a frame relay virtual circuit and the virtual circuit name and device name do not match.

USER LEVEL AUTHENTICATION
This parameter allows you to enable or disable user level authentication for this device. When user level authentication is enabled, the device is required to fulfill the necessary requirements of an off-node user level authentication server, such as RADIUS, ACE, or TACACS, after being authenticated at the device level.

IP HOST IDENTIFIER
The IP Host Id is used to authenticate a device over the IP Host (RFC 1294) line protocol. A unique identifier, 1 to 24 non-blank characters in length, it identifies the device. This identifier is exchanged and validated when the device connects to the system. This identifier must be identical to the identifier configured on the device's IP Host system. This field is only required when the IP routing operating mode is enabled. The identifier entered here must be identical to the configured identifier for the device's remote IP Host device.

BRIDGE ETHERNET ADDRESS
This address is used for authentication purposes on connections made over the HDLC Bridge line protocol. It is required if Bridge Ethernet Address Security is enabled.

This is the MAC address of the remote bridge device. This value is passed to the system (in band) when a connection is established. The system will look up the incoming Bridge Ethernet Address in the On-node Device Table. If the address is not included in the On-node Device Table, the system will reject the incoming call. If the address is included in the On-node Device Table, and the corresponding device entry is not configured with a bridge password, the connection will be established. If the address is included in the On-node Device Table, and the corresponding device entry is configured with a bridge password, the system will validate the password before establishing the connection.

BRIDGE PASSWORD
This password is used by the HDLC Bridge line protocol. It is an unencrypted password value (a string of 1 to 12 characters) used as a secondary security check when Bridge Ethernet Address Security is enabled. Its use is optional; however, if it is specified, it must be correct for the connection to be allowed. This value is passed to the system (in band) when an incoming call is received. The system compares the incoming password with the value found in the On-node Device Table. If the incoming password matches the associated On-node Device Table Bridge password, the connection is established. Otherwise, the system will reject the incoming call.

This value is stored in the same location as the PAP password, so a change to one password affects the other.

CALLING LINE IDENTIFIER (CLID)
Applicable to ISDN connections only, and only when the CLID option is enabled. You can specify eight CLIDs for each device entry. Each CLID for a given device must be unique. This is the telephone number of the calling party that is connecting to the system. In some areas this information is passed to the system on the ISDN incoming connection message. The system will

compare the incoming CLID with the value configured in the On-node Device Table. If the numbers are identical the connection will be established. Otherwise, the system will reject the incoming call.

When two remote devices share the same line (a single point-multipoint ISDN line), they can also configure the same CLIDs if they both also have some other type of authentication configured (for example, PAP, CHAP, or Bridge MAC Address Authentication).

Note: If a system is brought on line with a device that has a required CLID that is a duplicate of another device's CLID, and no other type of authentication is used, a warning message is logged at initialization.So every attempt to connect the device thereafter will result in an error message being logged and the call being rejected.

IP Information Configuration Elements

IP Address

The device's IP address, if any, on the WAN link connecting it to the CyberSWITCH. Options are: none (for Direct Host or WAN links that plan to use dynamic address allocation), 0.0.0.0 (for unnumbered WAN links), or an explicitly defined IP address.

The system must have a valid IP Network Interface defined for this IP address. When IP dial-out is used, this address is required by the IP routing system in order to map the IP address to the phone number to be dialed.

Enable/Disable IP Routing

You may enable or disable IP routing on a per-device basis.

Enable/Disable Make Calls for IP Data

This element must be enabled to allow IP dial-out to function. At least one Dial-Out phone number or X.121 address is required to dial out.

IPX Information Configuration Elements

IPX Routing

You may enable or disable IPX on a per-device basis.

Make Calls for IPX Data

Indicates whether the system should establish a WAN connection in order to forward IPX datagrams to this remote device. If enabled, at least one Dial-Out phone number or X.25 VC name is required.

IPXWAN protocol

Indicates that the remote device is an IPX router and that the IPXWAN protocol must immediately succeed IPXCP negotiations. Provides interoperability with Novell products.

IPX routing protocol

Indicates the protocol the remote device will be using to communicate with the CSX system:

- none
- RIP/SAP
- triggered RIP/SAP

IPX EXTERNAL WAN NETWORK NUMBER
Specifies a user-configurable IPX external network number on the WAN (necessary with CSX200 and CSX400 platforms only). This parameter can be a hexadecimal value from 1 to 4 bytes in length.The default value is *none*.

WAN PEER TYPE
Specifies an active WAN peer (receives and sends information at all times) or a passive WAN peer (receives / sends information only when a connection is up). In order for an active peer type to work properly, the *Make Calls* field must also be enabled.

SPOOFING OPTIONS
Spoofing allows you to prohibit excessive ISDN connections by internally generating a desired response packet when a request packet is received that should be routed over the WAN and there is no connection up to the remote device. Refer to *IPX Spoofing* for a description of available options.

APPLETALK INFORMATION CONFIGURATION ELEMENTS

APPLETALK ADDRESS
The AppleTalk address of this device (remote device).

If the device communicates using a numbered point-to-point link, then the address must belong to an AppleTalk network to which one of our WAN ports connects.

If the device communicates using an unnumbered point-to-point link, the WAN UnNumbered port must be configured and the address must be 0.0.

If the device is over a MAC dial-in port, no AppleTalk address needs to be entered. The device is assigned a random AppleTalk address within the specifications of the MAC dial-in port configuration each time it connects. However, if you choose to provide an AppleTalk address for the device, this address will be assigned to the MAC dial-in port device each time it connects.

ENABLE / DISABLE APPLETALK ROUTING
This parameter indicates whether the remote device routes AppleTalk datagrams or not. When enabled, it indicates that the remote device will route AppleTalk datagrams. When disabled, it indicates that the remote device will bridge AppleTalk datagrams. Note that it requires AppleTalk RLAN feature to handle bridged AppleTalk datagrams, and therefore until AppleTalk RLAN is implemented, AppleTalk routing can not be used with remote devices that do not route AppleTalk.

ENABLE / DISABLE MAKE CALLS FOR APPLETALK DATA
Indicates whether AppleTalk dial out to this device is allowed or not.

APPLETALK ROUTING PROTOCOL
Specifies what routing protocol the system should use with this remote device. Since RTMP periodically sends out routing updates, *RTMP* should be chosen only when the remote device is connected over the WAN links whose cost is not a major concern, such as dedicated links. The default value is *None*.

BRIDGE INFORMATION CONFIGURATION ELEMENTS

IP (SUB) NETWORK NUMBER

If the CyberSWITCH uses an IP RLAN interface to connect to a remote bridge, you must provide this information.

This address associates the bridge with the IP network to which it connects. Enter this address using dotted decimal notation. This parameter applies to the network-portion of the IP address only. Note that if you change the IP address under the *IP information* menu selection, this parameter will reflect that change.

ENABLE / DISABLE BRIDGING

You may enable or disable bridging on a per device basis. You must enable bridging for remote LAN devices, which indicates that the remote device is a bridge and not a router.

MAKE CALLS FOR BRIDGE DATA

You must enable this element to allow bridge dial out to function. You must also complete the following configuration:

- Enable bridging at the system level and at the per-device level.
- Either add the device to the CyberSWITCH's Known Connect List, or configure a bridge connection filter. For information regarding the Known Connect List, refer to page 285. For information regarding bridge filters, refer to page 269.

Note: This feature is not yet supported for IPX Remote LANs.

IPX REMOTE LAN NETWORK NUMBER

If the CyberSWITCH uses an IPX RLAN interface to connect to a remote bridge, you may choose to change this information.

This parameter associates the bridge with the IPX network to which it connects. Enter the IPX external network number of the remote LAN, or accept the default value of *none*.

If this parameter remains *none*, the CyberSWITCH will assume the network number is that of the first configured IPX Remote LAN interface. This is convenient in applications in which remote LANs consist only of clients (thus no explicit external network address), all of which are on the same external virtual LAN.

If you choose to change this parameter, you must specify the IPX external network number used on the remote LAN in question. This value must be the same as the value configured for the corresponding IPX Remote LAN interface.

IPX SPOOFING OPTIONS

Note: This feature is not yet supported for IPX Remote LANs. Do not attempt to configure.

APPLETALK NETWORK NUMBER

If the CyberSWITCH uses an AppleTalk WAN (Remote LAN) port to connect to a remote bridge, you may choose to change this information.

This parameter associates the bridge with the AppleTalk network to which it connects. Enter the AppleTalk network number / range (which corresponds to a configured AppleTalk Remote LAN port), or accept the default value of *none*. If this parameter remains *none*, the CyberSWITCH will assume an association with the first configured AppleTalk Remote LAN port.

COMPRESSION CONFIGURATION ELEMENTS

DEVICE COMPRESSION STATUS
Allows you to enable or disable compression for the individual device. If this option is enabled, then the CyberSWITCH will negotiate compression with this device. Otherwise, the system will not negotiate compression with this device, leaving the compression resources available for other devices. When adding a new device, this option derives its value from the default device compression option.

Note: Currently applies only to devices which connect using the PPP protocol.

STARTING PPP STAC- LZS SEQUENCE NUMBER
When using the PPP compression with the STAC-LZS protocol, certain devices may not adhere to the protocol specification's requirement that sequence numbers begin with 1, resulting in a resynchronization sequence on the first frame which is exchanged. When the peer fully supports the CCP protocol's Reset mechanism, this will only result in the minor inconvenience of a lost frame at the beginning of a session. However, if such a device's resynchronization mechanism is to completely renegotiate CCP (as has been witnessed in testing with some vendors' devices), this sequence will repeat infinitely.

This option provides a way to override the starting sequence number used when connecting to such devices. When adding a new device, this option derives its value from the system-wide Starting PPP STAC-LZS Sequence Number, presented previously in the system-wide compression configuration section. In the majority of cases, it will not be necessary to modify this value.

As its name implies, this option is only used when the device connects using the PPP protocol.

ON-NODE DEVICE DATABASE BACKGROUND INFORMATION

The On-node Device Table is a set of valid devices that can access the network resources connected to the system. The On-node Device Table contains a symbolic name for the device and a unique identifier that is used to enforce device security. The On-node Device Table is referenced when at least one device level system security option is enabled.

ON-NODE DEVICE DATABASE SECURITY REQUIREMENTS

The following sections provide the On-node Device Table configuration requirements for possible security option configurations for each category of remote device. Categories are defined by the operating mode (bridging or routing), and the line protocol in use.

Bridging with HDLC Bridge Devices

To allow a Bridge device to connect to the CyberSWITCH, you must have MAC Layer Bridging enabled. For each HDLC bridge device using this type of connection, you may need to enter the Device Name, Calling Line Id, Remote Bridge Ethernet Address, and Password.

The following table identifies the configuration requirements for possible security options for remote bridge devices.

Security Mode Configuration		*On-node Device Table Configuration Data*		
Calling Line Id	*Bridge Ethernet Address*	*Calling Line Id*	*Bridge Ethernet Address*	*Bridge Password*
Enabled	Disabled	Required	Not Requested	Not Requested
Disabled	Enabled	Not Requested	Required	Optional per device entry
Enabled	Enabled	Conditionally Required*	Conditionally Required*	Optional per device entry (if entry specifies an Ethernet Address)

**Conditionally Required* means you must specify at least one of either the Calling Line Id or the Ethernet Address. You may specify both.

IP Routing with HDLC Bridge Devices

To allow devices to connect to the CyberSWITCH using IP routing through a Bridge device, you must configure a RLAN Interface. IP routing must also be enabled. For each HDLC Bridge using this type of connection, you may need to enter the Device Name, Calling Line Id, Remote Bridge Ethernet Address, Bridge Password, and IP (Sub) Network Number.

The following table identifies the configuration requirements for possible security options for IP Routing with Bridge Devices.

Security Mode Configuration		*On-node Device Table Configuration Data*			
Calling Line Id	*Bridge Ethernet Address*	*Calling Line Id*	*Bridge Ethernet Address*	*Bridge Password*	*IP (Sub) Network Number*
Enabled	Disabled	Required	Not Requested	Not Requested	Required if only IP Routing is Enabled
Disabled	Enabled	Not Requested	Required	Optional per device entry	Required if only IP Routing is Enabled
Enabled	Enabled	Conditionally Required*	Conditionally Required*	Optional per device entry (if entry specifies an Ethernet Address)	Required if only IP Routing is Enabled

**Conditionally Required* means you must specify at least one of either the Calling Line Id or the Ethernet Address. You may specify both.

IP Routing with IP Host Devices (RFC1294)

To allow an IP Host device to connect to the CyberSWITCH, you must have IP Routing and IP Host Security enabled. For each IP Host device using this type of connection, you may need to enter the device's IP address, IP Host Id, and Calling Line Id.

The following table identifies the configuration requirements for possible security options for IP Host devices.

Security Mode Configuration		*On-node Device Table Configuration Data*		
Calling Line Id	*IP Host Id*	*Calling Line Id*	*IP Host Id*	*IP Address*
Disabled	Enabled	Not Requested	Required	Required
Enabled	Enabled	Optional per device entry	Required	Required

IP Routing with PPP IP Devices (Using IPCP)

To allow a PPP IP device to connect to the CyberSWITCH, you must have IP routing enabled. For each PPP IP Device using this type of connection, you may need to enter the device's IP address, a PAP Password or a CHAP Secret, and Calling Line Id.

The following table identifies the configuration requirements for possible security options for PPP IP Devices.

Security Mode Configuration		*On-node Device Table Configuration Data*		
Calling Line Id	*PAP or CHAP Security*	*Calling Line Id*	*PAP Password or CHAP Secret*	*IP Address*
Disabled	Enabled	Not Requested	Required	*Required
Enabled	Enabled	Optional per device entry	Optional	*Required
Enabled	Disabled	Required	Optional	Optional

*Required: An IP address is required if the remote device does not support IP address negotiation. When the remote device does support IP address negotiation, an IP address is not required.

Note: If CHAP Security is enabled, and Outbound Authentication has not been disabled, a CHAP Secret must be entered for both the remote device and for the CyberSWITCH. Refer to *System Information* for information regarding the System Secret. If Outbound Authentication has been disabled, a CHAP Secret is not required for the remote device.

Bridging with PPP Bridge Devices (Using BCP)

To allow a PPP Bridge device to connect to the CyberSWITCH, you must have Bridging enabled. For each PPP Bridge device using this type of connection, you may need to enter a PAP Password or a CHAP Secret, and a Calling Line Id.

The following table identifies the configuration requirements for possible security options for PPP Bridge Devices.

Security Mode Configuration		*On-node Device Table Configuration Data*	
Calling Line Id	*PAP or CHAP Security*	*Calling Line Id*	*PAP Password or CHAP Secret*
Disabled	Enabled	Not Requested	Required
Enabled	Enabled	Optional per device entry	Required
Enabled	Disabled	Required	Optional

Note: If CHAP Security is enabled, and Outbound Authentication has not been disabled, a CHAP Secret must be entered for both the remote device and for the CyberSWITCH. Refer to the *System Information* for information regarding the System Secret. If Outbound Authentication has been disabled, a CHAP Secret is not required for the remote device.

IP Routing with PPP Bridge Devices (Using BCP)

To allow devices to connect to the CyberSWITCH using IP routing through a PPP Bridge device, you must configure a RLAN IP Network Interface. IP routing must also be enabled. For each PPP Bridge using this type of connection, you may need to enter the Device Name, a Calling Line Id, a PAP Password or a CHAP Secret, and an IP (Sub) Network Number.

The following table identifies the configuration requirements for possible security options for IP Routing with PPP Bridge Devices.

Security Mode Configuration		*On-node Device Table Configuration Data*		
Calling Line Id	*PAP or CHAP Security*	*Calling Line Id*	*PAP Password or CHAP Secret*	*IP (Sub) Network Number*
Disabled	Enabled	Not Requested	Required	Required if only IP Routing is Enabled
Enabled	Enabled	Optional per device entry	Required	Required if only IP Routing is Enabled
Enabled	Disabled	Required	Optional	Required if only IP Routing is Enabled

Note: If CHAP Security is enabled, and Outbound Authentication has not been disabled, a CHAP Secret must be entered for both the remote device and for the CyberSWITCH. Refer to *System Information* regarding the System Secret. If Outbound Authentication has been disabled, a CHAP Secret is not required for the remote device.

OFF-NODE DEVICE DATABASE LOCATION

CONFIGURING OFF-NODE DEVICE DATABASE LOCATION

USING CFGEDIT

1. Select *Off-node Device Database Location* from the Device Level Databases menu. If you need guidance to find this menu, refer to the instructions provided in the *On-node Device Database* configuration section. The following screen will be displayed:

```
Off-node Device Database Location Menu:

   1) None (Use On-node)
   2) CSM
   3) RADIUS

Current Off-node Device Database Location is "None (Use On-node)".

Select function from above or <RET> for previous menu:
```

2. Select the location of the off-node device database, or select None in order to use the on-node device database.

OFF-NODE DEVICE DATABASE LOCATION CONFIGURATION ELEMENTS

DATABASE LOCATION
The database location for device level security. The choices for the off-node database location are None (Use on-node), CSM, or RADIUS. Choosing an off-node database location enables the particular database.

Note: Enabling CSM as the off-node device database location automatically enables CSM as a Call Control Manager. However, disabling CSM as the authentication agent will not disable CSM as a Call Control Manager. Refer to the *SecureFast Virtual Remote Access User's Guide* or the *Configuring Call Control* chapter of this guide for more information.

OFF-NODE DEVICE DATABASE LOCATION BACKGROUND INFORMATION

An off-node, central database allows a network with more than one CyberSWITCH to access one database for device authentication. The CyberSWITCH will access the off-node database to locate authentication information on a remote device that is attempting to establish a connection.

If the On-node Device Database has been enabled, and either CSM or RADIUS has been selected as the off-node database location, both databases will be searched for the device attempting the incoming or outgoing call. The on-node database will be searched and then, if the correct device is not found, the off-node database will be searched. Authentication is based on device information received from the first matching database. Matching a device is defined in different ways, depending on the call is made. For example, if an outbound call is made on an IP WAN interface by using the ip ping command, the IP address is the method that is used to search the database. If a matching IP address is found, a connection is attempted. If the system is unable to authenticate the peer, the connection attempt is done. The system will not attempt to continue searching the remaining database entries or additional off-node database for the correct peer.

CONFIGURING USER LEVEL DATABASES

OVERVIEW

User level security is an authentication process between a specific user and a device. The authentication process is interactive; users connect to a terminal server and need to interact with it in order to communicate with other devices beyond the server. The CyberSWITCH supports user level security through the RADIUS, TACACS, or ACE Server.

This chapter provides information for enabling an off-node user level database. Refer to the chapter *Configuring Off-node Server Information* for configuration instructions for specific servers.

USER LEVEL AUTHENTICATION DATABASE LOCATION

CONFIGURING AUTHENTICATION DATABASE LOCATION

USING CFGEDIT

1. Select *Security* from the main menu.

2. Select option (4), *User Level Databases (Enable/Disable)* from the Security Menu. The following screen be displayed:

```
User Level Databases Menu:

Authentication Database Location:         Status         Telnet Port
-------------------------------------------------------------------

   1) RADIUS Authentication Server        ENABLED        7001
   2) TACACS Authentication Server        ENABLED        7000
   3) ACE Authentication Server           ENABLED        7003

Select function from above or <RET> for previous menu:
```

3. Select the option you wish to configure and press <RET>. This prompt acts like a toggle switch. If you select a server that is currently enabled, the system will prompt you to disable it. If you select a server that is currently disabled, follow the onscreen instructions to enable the server, including entering the Telnet port number for the server. If you answer yes, you will need to provide the Telnet port number.

USING MANAGE MODE

seclevel
Displays the current security level configuration data.

USER LEVEL AUTHENTICATION DATABASE LOCATION CONFIGURATION ELEMENTS

DATABASE LOCATION
The database location for user level security. Choices are: RADIUS Server, TACACS Server, or ACE Server.

DATABASE TELNET PORT NUMBER
You must also specify the Telnet port number to be used for authentication with the selected server. This port number is a unique number that identifies the server. For remote authentication, users will need to Telnet into this specially configured port. Any Telnet sessions coming through this port must be authenticated via the specified Authentication Server before other actions are allowed.

Note: For user level security, the CyberSWITCH's default Telnet port number is 7000, not the normal default (23). The Telnet port number used for remote administration sessions is the 23. If you wish, you can reconfigure the port numbers so that these values are switched (i.e., the Telnet administration session uses a higher number, user level security uses the normal default of 23), but you cannot use 23 for both.

USER LEVEL AUTHENTICATION DATABASE LOCATION BACKGROUND INFORMATION

An off-node, central database allows a network with more than one CyberSWITCH to access one database for user authentication. The CyberSWITCH will access the off-node database to locate authentication information on a user that is attempting to establish a connection. If the user's information matches what is configured in the database, then the connection is allowed.

CONFIGURING OFF-NODE SERVER INFORMATION

OVERVIEW

This chapter provides information on configuring the CyberSWITCH so that it will be able to communicate with an off-node server. This communication may be for Authentication or Accounting purposes. The off-node servers supported are:

- Connection Services Manager (CSM)
- RADIUS
- TACACS
- ACE

CSM, RADIUS Authentication, TACACS and ACE are all authentication servers; RADIUS Accounting is the accounting server. Please refer to your specific off-node server documentation for information on each server's individual requirements.

This chapter also provides off-node configuration information for:

- Multiple administration login names
- RADIUS Accounting
- RFC2138 RADIUS
- Dynamic Device options

MULTIPLE ADMINISTRATION LOGIN NAMES

When configuring the off-node server itself, you may configure up to 101 different names for *system administration login*. You may assign administration capabilities to specific personnel with different passwords, passcodes, and / or SecureID cards. By using this feature, you can track who logged in to what system via the security server log.

When configuring your off-node server, identify each device and / or user with one of the following access levels:

- *guest*: limited access
- *admin*: administrative-level access when only one administrator necessary
- *admin00 through admin99*: administrative-level access for multiple users

An example of a properly configured ACE server may resemble the following:

User
name: *John Doe*
address: *Remote Office1*
client activation: *mynode1*
default login name: *admin10*
assigned token: *04690074*

Client
name: *mynode1*
address: *1.1.1.1*
type: *communications server*
user activation: *John Doe*

CSM AUTHENTICATION SERVER

CONFIGURING CSM AUTHENTICATION SERVER

Notes: In order for the CyberSWITCH to reference CSM for device authentication, the following configuration steps must first be completed:

- IP Routing must be enabled. If you try to enable CSM before IP routing has been enabled, an error message will be displayed.
- The appropriate LAN network interface(s) must be configured to represent the local IP network.
- The appropriate WAN network information must be configured for each type of remote device configured that will connect to the system.

If you have configured Call Restrictions, you have configured system wide Call Restrictions. System wide Call Restrictions will override Call Restrictions configured on CSM on a per device basis.

USING CFGEDIT

1. Select *Security* from the main menu.

2. Select option (5), *Off-node Server Information* from the Security Menu. The following screen is displayed:

```
Off-node Server Information Menu:

   1) CSM
   2) RADIUS
   3) TACACS
   4) ACE

Select function from above or <RET> for previous menu: 1
```

3. Select *CSM* from the Off-node Server Information Menu. The following screen is displayed:

```
CSM Menu:

           TCP Port Number             is 2000

CSM Server Options:
   1)  CSM TCP Port

Select function from above or <RET> for previous menu: 1
```

4. Enter the TCP port number used by CSM.

USING MANAGE MODE COMMANDS

csm
Displays the current CSM configuration data.

csm change
Allows you to change the CSM TCP port number.

CSM AUTHENTICATION SERVER CONFIGURATION ELEMENTS

TCP PORT NUMBER
The TCP port number used by CSM. Note that you can assign a device-defined port number, but that the CSM TCP port number must be entered identically on both the CyberSWITCH and CSM.

CSM AUTHENTICATION SERVER BACKGROUND INFORMATION

When a remote site calls a CyberSWITCH, it sends its identification (such as the system name) and a password (or challenge). The system then sends the data in a message to CSM on a TCP connection. CSM will find the device in its database, searching for the system name (if provided) or the Ethernet address for Combinet Proprietary Protocol (CPP) devices. After finding the device, the password or challenge is verified, and configuration information about the device is sent to the system.

Before allowing data to be sent to the newly-connected device, the system will again query CSM, this time to verify if the call is acceptable. CSM checks against various configuration settings to see if the call is to be allowed.

RADIUS SERVER

You may use the RADIUS Server as an *Authentication Server*, an *Accounting Server*, or both. Refer to the following sections for details on configuring these off-node servers.

CONFIGURING A RADIUS AUTHENTICATION SERVER

Notes: In order for the CyberSWITCH to reference a RADIUS Server, ensure the following:

- IP Routing must be enabled. If you try to enable the RADIUS Server before IP routing has been enabled, an error message will be displayed.
- The appropriate LAN network interface(s) must be configured to represent the local IP network.
- The appropriate WAN network information must be configured for each type of remote device configured that will connect to the system.
- The system must have a valid route to the RADIUS Server. This route can be via a directly connected network interface or via a static route. If the RADIUS Server has a direct physical connection to the network, the appropriate network interface must then be configured for that connection. If the RADIUS Server has no direct physical connection to the network, then a static route needs to be configured to establish a route, with one exception: if the router connecting the system to the RADIUS Server supports RIP, no static route is needed. If there are multiple CyberSWITCHes at one site, it is more convenient to maintain all of the static route information for these systems on a central RADIUS Server. The static routes then do not need to be duplicated on all of the Cabletron systems. This is done by enabling the “IP Routes via RADIUS” feature available under CFGEDIT’s IP Information Menu, and including a Framed Route attribute for each system’s RADIUS device entry.

For Device Level Security:
- Specify Device Level Security (from *Main Menu, Security, Security Level*)
- Select RADIUS from *Off-Node Device Database Location* (*Main Menu, Security, Device Level Databases*)

For User Level Security:
- Select User Level Security (from *Main Menu, Security, Security Level*)
- Enable RADIUS Authentication Server (from *Main Menu, Security, User Level Databases*)

If you are using an *RFC2138 RADIUS* Server, you must reflect this correctly under *Main Menu, Security, Off-node Server Information, Misc Off-node Server Options*.

USING CFGEDIT

1. Select option (2), *RADIUS* from the Off-node Server Information menu. If you need guidance to find this menu, refer to the instructions provided in the *CSM Authentication Server* configuration section. The following screen will be displayed:

```
RADIUS Authentication Server Menu:

         Primary Server
           IP Address                  is 128.111.011.001
           Shared Secret               is "SHAREDSECRET1234"
           UDP Port Number             is 5800

         Secondary Server
                                       is Not Configured
         Access Request Retry
           Number of Access Retries    is 5
           Time between Retries        is 2 seconds

RADIUS Server Options:
   1) Primary (Master) Server
   2) Secondary (Slave) Server
   3) Miscellaneous Information

Select function from above or <RET> for previous menu:
```

2. Select (1) *Primary Server* to enter the following information:
   a. IP address of the Authentication Server
   b. shared secret between the CyberSWITCH and Authentication Server
   c. UDP port number used by the Authentication Server

3. Optional: configure a secondary RADIUS Server with selection (2). In the event that the primary server does not respond to system requests, the secondary server will be queried for device authentication information. The address of the Secondary RADIUS Server must not be the same as the Primary RADIUS Server.

4. Select *Miscellaneous Information* to finish the configuration. Specify the number of access request retries that the system will send to the Authentication Server, as well as the time between retries.

USING MANAGE MODE COMMANDS

radius
Displays the current RADIUS server configuration data.

radius change
Allows you to change the current RADIUS server configuration data. After entering the *radius change* command, you will be prompted for the configuration elements you want to change.

RADIUS AUTHENTICATION SERVER CONFIGURATION ELEMENTS

IP ADDRESS
The IP address in dotted decimal notation for the RADIUS Server. This information is required for the Primary RADIUS Server, and also required if a Secondary RADIUS Server is configured. If a Secondary RADIUS Server is configured, it must have a different IP address than the Primary RADIUS Server.

SHARED SECRET
The shared secret can be 1 to 16 characters in length. Any ASCII character may be used. The same shared secret is configured on the CyberSWITCH and the RADIUS Server. It is used for security purposes. As opposed to a password, a shared secret is not sent across lines, and therefore is not susceptible to interception. Instead, a calculation is done on the packets transmitted between the two devices, and the results are compared to the shared secret for validation. The shared secret between the CyberSWITCH and the selected server secures the access to both devices. Both devices must know the shared secret before any exchange of information can take place. If the calculation's results do not match the shared secret, the connection is terminated.

The RADIUS server maintains a list of all the system's services, which includes an entry for each System's IP address and associated shared secret.

UDP PORT NUMBER
The UDP port number used by the RADIUS Server. This information is required for the Primary RADIUS Server, and also required if a Secondary RADIUS Server is configured. The default value of 1645 is almost always used.

NUMBER OF ACCESS REQUEST RETRIES
The number of Access Request Retries that the system will send to the RADIUS Server. The initial default value is 3. The acceptable range is from 0 to 32,767.

TIME BETWEEN ACCESS REQUEST RETRIES
The time between Access Request Retries sent from the system. The initial default value is 1. The acceptable range is from 1 to 10,000.

RADIUS AUTHENTICATION SERVER BACKGROUND INFORMATION

If you require a central database for device authentication (capable of servicing several CyberSWITCHes), you can use an industry standard authentication server. The Remote Authentication Dial-In User Service (RADIUS) serves this purpose for both device level and user level security on the CyberSWITCH. The RADIUS Server can also be used to authenticate an administrative session.

The Remote Authentication Dial-In User Service (RADIUS) is a central database supported by the CyberSWITCH. RADIUS operates using two components: an authentication server and client protocols. The RADIUS Server software is typically installed on a UNIX-based or NT-based system that is local to the network. The client protocols allow the CyberSWITCH to communicate with the RADIUS server, ultimately authenticating devices.

When enabled and properly configured, the CyberSWITCH software implements the RADIUS client. The RADIUS client sends packets to the RADIUS Authentication Server. These packets support the following attributes:

- User-Name
- NAS-IP-Address
- CHAP or PAP password
- Framed-Protocol
- Called-Station-Id
- Calling-Station-Id

The following is a typical scenario if the RADIUS Server is activated: when a remote device needs to be authenticated, the system will send an access request to the primary RADIUS Server. After the configured time interval the system will send an access request retry if the primary server does not respond. After the configured number of retries, the system will request authentication information from the secondary server if one is configured. The connection will be released if neither server responds to the access requests.

The section titled *On-node Device Table Security Requirements* describes the device authentication information required for each type of remote device. The information you need to configure depends upon what you have configured for the CyberSWITCH operating mode (bridging and / or routing), and the security options you select.

To configure the RADIUS Server itself, refer to the *RADIUS Authentication Server User's Guide*. If you have Internet access, you may obtain this guide by following the steps outlined below:

- Use your Web browser to get to the following address: *http:// service.nei.com*
- From the resulting screen, click on *Anonymous*.
- Click on the *Radius* directory.
- Click on the *Docs* directory. The guide will be under this directory.

CONFIGURING A RADIUS ACCOUNTING SERVER

Refer to the *preliminary steps* described in *Configuring a RADIUS Authentication Server*. These also apply to RADIUS Accounting.

USING CFGEDIT

1. From CFGEDIT Main Menu, select *(3) Security*.
2. Select *(5) Off-node Server Information*.
3. Select *(5) RADIUS Accounting*. A screen similar to the following will display:

```
RADIUS ACCOUNTING Menu:

         Primary (Master) Server
           IP Address                  is 010.000.000.108
           Shared Secret               is “ralph”
           UDP Port Number             is 1813

         Secondary (Slave) Server
                                       is Not Configured
         Access Request Retry
           Number of Access Retries    is 3
           Time between Retries        is 1 second

RADIUS Accounting Server Options:
   1) Primary (Master) Server
   2) Secondary (Slave) Server
   3) Miscellaneous Information

Select function from above or <RET> for previous menu:
```

4. Select (1) *Primary Server* to enter the following information:
   a. IP address of the Accounting Server
   b. shared secret between the CyberSWITCH and Accounting Server
   c. UDP port number used by the Accounting Server

5. Optional: configure a secondary RADIUS Accounting Server. In the event that the primary server does not respond to system requests, the secondary server will be used for accounting information. The address of the Secondary RADIUS Server must not be the same as the Primary RADIUS Server.
6. Select *Miscellaneous Information*. Specify the number of retries that the system will use with the Accounting Server, as well as the time between retries.
7. Return to the *Off-node Server Information* Menu.
8. Select *Misc Off-node Server Options.* A screen similar to the following will display current settings:

```
Misc Off-node Server Options Menu:
                                            Current Settings
   1) Radius Accounting (Enable/Disable)    Enabled
   2) Radius Type (RFC2138/Cabletron)       RFC2138 compliant
   3) Dynamic Device Option (Enable/Disable) Enabled
   4) Dynamic Device Default Settings

Select function from above or <RET> for previous menu:
```

9. Verify that RADIUS Accounting is enabled. If enabled, press <RET> to exit the menu. If disabled, select the RADIUS Accounting function to enable the feature. (This selection is a simple toggle switch).

USING MANAGE MODE COMMANDS

offnode

Allows you to change current settings for off-node server options. You may use this command to enable the RADIUS Accounting feature.

`radius`
Displays the current RADIUS server configuration data.

`radacc`
Allows you to change the current RADIUS Accounting Server configuration data. After entering the `radacc` command, you will be presented with a RADIUS Accounting Menu similar to that in CFGEDIT.

RADIUS Accounting Server Configuration Elements

RADIUS Accounting
You may enable or disable this feature. The default is *disabled*.

UDP Port Number
The UDP port number used by the RADIUS Accounting Server. This information is required for the Primary RADIUS Server, and also required if a Secondary RADIUS Server is configured. The officially-assigned port number for RADIUS Accounting is 1813.

Refer to the *RADIUS Authentication Server Configuration Elements* section for additional elements that are in common with the RADIUS Authentication Server.

RADIUS Accounting Server Background Information

CyberSWITCH UAA software version 7.2 (or earlier) provides for a RADIUS implementation which uses RADIUS *only for Authentication*. CyberSWITCH UAA software version 7.3 (and beyond) provides the ability to use RADIUS *to maintain accounting information* as well. This additional capability should be especially useful to Internet Service Providers who have standardized on RADIUS for call accounting.

When enabled and properly configured, the CyberSWITCH software implements a RADIUS Accounting Client. The RADIUS Accounting Client sends accounting packets to the RADIUS Accounting Server. These packets support the following attributes:

- NAS-IP-Address
- NAS-Port-Type (in format ***abcdd,*** where *a* = WAN card slot, b=WAN port, *c* = modem card slot, and *dd* = modem number)
- Acct-Status-Type
- Acct-Session-Id
- User-Name
- Calling-Station-Id
- Framed-IP-Address
- Acct-Session-Time

When a call is initiated and authenticated successfully, CyberSWITCH software will send an accounting-request packet to flag a call "START". When the call is terminated, it will send an accounting-request packet with a value of "STOP". This packet exchange provides a means of determining the session time for the call (i.e., the number of seconds that the call has been active).

Performance

RADIUS Accounting consumes an additional 32 bytes of memory per connection, or a total of 6144 bytes on a full, 192-connection system.

VERIFICATION AND DIAGNOSIS

After configuring the RADIUS Accounting Server, connect via a dial-in client, and then disconnect. On the RADIUS Accounting Server, verify that it has received the Accounting Start and Stop message. If it has not, check the CyberSWITCH system log. If there is a message that no response was received from the Accounting Server, then verify your configuration.

To verify configuration, use CFGEDIT and check:

- is RADIUS Accounting enabled (*Security, Off-node Server Information, Misc options*)?
- correct IP address (*Security, Off-node Server Information, RADIUS Acctng*)?
- correct shared secret?
- correct UDP port number?

To determine if you have communications with the RADIUS Accounting Server, issue the `IP ping x.x.x.x` command, where `x.x.x.x` is the RADIUS Accounting Server's address.

If this test fails on occasion, yet is successful at other times, it may be that the connection between the CyberSWITCH and the RADIUS Accounting Server is inadequate to provide reasonable accounting information.

RADIUS RFC2138

In addition to the Cabletron implementation of RADIUS (which supports dialout), the CyberSWITCH also supports an RFC2138-compliant implementation. If you are using an RFC2138 RADIUS, be sure to enable this RFC2138 implementation.

ENABLING RADIUS TYPE

USING CFGEDIT

1. From CFGEDIT Main Menu, select *(3) Security*.
2. Select *(5) Off-node Server Information*.
3. Select *Misc Off-node Server Options*. A screen similar to the following will display current settings:

```
Misc Off-node Server Options Menu:
                                          Current Settings
   1) Radius Accounting (Enable/Disable)  Enabled
   2) Radius Type (RFC2138/Cabletron)     RFC2138 compliant
   3) Dynamic Device Option (Enable/Disable) Enabled
   4) Dynamic Device Default Settings

Select function from above or <RET> for previous menu:
```

4. Check the current setting for Radius type.
   Note: This selection toggles back and forth. If the current setting is RFC2138 compliant, you will enable the Cabletron implementation by selecting *Radius Type*. If you select *Radius Type* again, you will return the function to RFC2138 compliance.
5. Press <RET> to return to the previous menu.

USING MANAGE MODE

offnode

Allows you to change current settings for off-node server options. You may use this command to enable the RFC2138 compliance feature.

RADIUS TYPE CONFIGURATION ELEMENTS

RADIUS TYPE

Specify the type of RADIUS implementation: Cabletron implementation or RFC2138 implementation. For preexisting systems upgraded to UAA 7.3 software, the default is Cabletron implementation. For new systems shipped with 7.3 software, the default is RFC2138.

BACKGROUND INFORMATION

The Cabletron RADIUS implementation allows the CyberSWITCH to perform device lookups in RADIUS using MAC addresses, IP addresses, and other additional methods so that it can make outbound calls using RADIUS. However, this implementation does not conform to RFC2138, in which these "special" lookups are not permitted. The CyberSWITCH now provides an alternative implementation to conform to the RFC2138 standard. This RFC2138 option disables RADIUS lookups for outbound calls.

DYNAMIC DEVICE OPTION

This feature is specific to *Terminal Mode* configurations. Terminal Mode connections require both device-level + user-level security configurations. With the Dynamic Device Option, you no longer need to configure separate devices for each individual user. You may configure a single default device which will apply to every user dialing in and authenticating with RADIUS, ACE, or TACACS user-level security.

CONFIGURING THE DYNAMIC DEVICE OPTION

USING CFGEDIT

1. From CFGEDIT Main Menu, select *(3) Security*.
2. Select *(5) Off-node Server Information*.
3. Select *Misc Off-node Server Options.*
4. Check the current setting for *Dynamic Device Option*.
   Note: If enabled, press <RET> to exit the menu. If disabled, select the Dynamic Device Option function to enable the feature. (This selection is a simple toggle switch).
5. Return to the *Misc Off-node Server Options Menu.*
6. Select *Dynamic Device Default Settings.*
7. Provide a default device name.
8. Continue with the default device configuration just as you would for an on-node device entry. (For more information on device entries, refer to the *Current Device Table*.)

USING MANAGE MODE

offnode

Allows you to change current settings for off-node server options. You may use this command to enable and configure the dynamic device option.

DYNAMIC DEVICE CONFIGURATION ELEMENTS

DEVICE NAME

A 1 to 17-character, user-specified name. Any name may be entered. For dynamic devices, this name will not be used, but it must be entered to allow for creation of a device.

PAP PASSWORD

This password (a string of 1 to 12 ASCII characters) is used by PPP line protocol for PAP authentication. For dynamic devices, this password is not used unless the Outbound Authentication flag for the default device is enabled; but, *either the password or secret is required* regardless of the setting of the outbound authentication flag.

CHAP SECRET

This field (a string of 1 to 17 ASCII characters) is used by PPP line protocol for CHAP authentication. For dynamic devices, this secret is not used unless the Outbound Authentication flag for the default device is enabled; but, *either the password or secret is required* regardless of the setting of the outbound authentication flag.

OUTBOUND AUTHENTICATION

Since the main focus of this feature is ***not*** to require device-level authentication, the *Outbound Authentication* flag is disabled by default. However, if you would like to add additional security, you can enable outbound authentication for the default device. If this is the case, all terminal users dialing into the CyberSWITCH will need to pass user-level authentication, and configure their remote machines (i.e., *Win95 dialup client*) with:

- a user name that matches the name they will use for user-level security, and
- a password that matches the password / secret defined for the default device.

In this situation, everyone will have the same password / secret, but different names.

For more information on these and other device-level configuration elements, refer to *On-node Device Database Configuration Elements*.

BACKGROUND INFORMATION

Terminal Mode connections require both device-level + user-level security configurations. However, if you have a large number of users dialing in, you may not want to create an on-node or CSM database with devices for all possible users. If device-level authentication is not necessary, you can satisfy the device-level configuration requirement with the *dynamic device option*. This option allows the dynamic creation of devices, based on an authenticated user name, and with the device parameters associated with a “default” device. This “default” device is configured as part of the off-node server configuration. Configuration consists of enabling the dynamic device option, then specifying a PAP password or CHAP secret for the default device.

Once the dynamic device option is enabled, all terminal users dialing in will be given the same configuration parameters (such as IP enabled or disabled, etc.).

If a specific set of parameters is required for a particular device, configure the specific device independently, either locally (through the on-node device list) or in CSM. The CyberSWITCH will look at the configured device table first before proceeding to the dynamic device default configuration. Since the configured device table overrides the default configuration, leave the dynamic device option enabled, and configure specific devices for exceptional cases only.

TACACS AUTHENTICATION SERVER

CONFIGURING A TACACS AUTHENTICATION SERVER

Note: In order for the CyberSWITCH to reference the TACACS server, basic IP information must be configured. If the IP Host mode is not in use, you must also configure the following:

- a LAN Network interface must be configured appropriately for the IP network connected to each LAN port on the system
- at least one WAN Network Interface must be configured for TACACS to be operable

USING CFGEDIT

1. Select option (3), *TACACS* from the Off-node Server Information menu. If you need guidance to find this menu, refer to the instructions provided in the *CSM Authentication Server* configuration section. The following screen will be displayed:

```
TACACS Authentication Server Menu:

         Primary Server
           IP Address                  is 001.002.003.004
           UDP Port Number             is 49

         Secondary Server
           IP Address                  is 001.002.003.008
           UDP Port Number             is 49

         Access Request Retry
           Number of Access Retries    is 3
           Time between Retries        is 1 second
           TACACS Packet Format        is (ID CODE,PIN)

TACACS Server Configuration Options:
   1) Primary Server
   2) Secondary Server
   3) Access Request Retry

Select function from above or <RET> for previous menu:
```

2. Select (1) *Primary Server* to enter the following information:
   a. IP address of the Authentication Server
   b. UDP port number used by the Authentication Server

3. Optional: configure a secondary TACACS Server with selection (2). In the event that the primary server does not respond to system requests, the secondary server will be queried for device authentication information. The address of the Secondary Server must not be the same as the Primary Server.

4. Select (3) *Access Request Retry* to finish configuration. Specify the number of access request retries that the system will send to the Authentication Server, as well as the time between retries. You may also specify order of the TACACS authentication prompts for access request.

USING MANAGE MODE COMMANDS

tacacs
Displays the current TACACS off-node server configuration data.

tacacs change
Allows you to change the current TACACS off-node server configuration data. After entering the *tacacs change* command, you will be prompted for the configuration elements you want to change.

TACACS AUTHENTICATION SERVER CONFIGURATION ELEMENTS

IP ADDRESS
The IP address in dotted decimal notation for the TACACS Server.

UDP PORT NUMBER
The UDP port number used by the TACACS Server. The default value of 49 is almost always used.

NUMBER OF ACCESS REQUEST RETRIES
The number of Access Request Retries that the system will send to the TACACS Server. The initial default value is 3. The acceptable range is from 0 to 32,767.

TIME BETWEEN ACCESS REQUEST RETRIES
The time between Access Request Retries sent from the system. The initial default value is 1 second. The acceptable range is from 1 to 10,000.

TACACS PACKET FORMAT
The TACACS format for device authentication. The default format is ID code, PIN.

TACACS AUTHENTICATION SERVER BACKGROUND INFORMATION

The Terminal Access Controller Access Control System (TACACS) is a database supported by the CyberSWITCH. TACACS operates using two components: client code and server code. TACACS server software is installed on a UNIX-based system connected to the CyberSWITCH network. The client protocols allow the system to communicate with the TACACS server, ultimately authenticating devices.

The following is a typical scenario if the TACACS Server is activated: with user level security, a remote user will Telnet into a specified system port for user authentication. The system, in turn, will send an access request to the primary TACACS Server. After the configured time interval the system will send an access request retry if the primary server does not respond. After the configured number of retries, the system will request authentication information from the secondary server if one is configured. The connection will be released if neither server responds to the access requests.

Note: For user level security, the CyberSWITCH's default Telnet port number is 7000, not the normal default (23).

ACE AUTHENTICATION SERVER

CONFIGURING AN ACE AUTHENTICATION SERVER

Note: In order for the CyberSWITCH to reference an ACE server, the following configuration steps must first be completed:

- basic IP routing information must be configured for ACE
- a LAN Network interface must be configured appropriately for the IP network connected to each LAN port on the system
- at least one WAN Network Interface must be configured for ACE to be operable

After ACE configuration but before attempting to access the ACE Server, both the ACE Server and the CyberSWITCH need to agree upon a "secret." After configuring the ACE server on the CyberSWITCH, issue the `sentry ace` system command. This command will establish the necessary secret for communications between the two systems.

USING CFGEDIT

1. Select option (4), *ACE* from the Off-node Server Information menu. If you need guidance to find this menu, refer to the instructions provided in the *CSM Authentication Server* configuration section. The following screen will be displayed:

```
ACE Authentication Server Menu:

         Primary (Master) Server
                                      is Not Configured

         Secondary (Slave) Server
                                      is Not Configured

         Access Request
           Number of Access Retries    is 3
           Time between Retries        is 1 second
           Encryption Method           SDI
           Source IP address           is Not Configured

ACE Server Options:
   1) Primary (Master) Server
   2) Secondary (Slave) Server
   3) Miscellaneous Information
   4) Load ACE configuration file.

Select function from above or <RET> for previous menu: 1
```

2. Select *Primary Server* and enter the following information:
   a. IP address of the Authentication Server
   b. UDP port number used by the Authentication Server

3. If your configuration includes an ACE Slave server, then select *Secondary Server*. Enter its IP address. The UDP port number for the Master and Slave servers will be the same, regardless of which server configuration screen from which it is entered.

4. Select *Miscellaneous Information* to finish the configuration.
   a. Specify the number of access request retries that the system will send to the Authentication Server.

b. Specify the time between retries.
c. Choose between the DES or SDI Encryption Method. The algorithm you select must be compatible with the ACE Server setup.
d. You will also be prompted for a source IP address. This source IP address should be a valid address for the CyberSWITCH. The IP address must match the IP address listed for the system in the ACE Server host machine's `/etc/hosts` file.

USING MANAGE MODE COMMANDS

`ace`
Displays the current ACE Server configuration data.

`ace change`
Allows you to change the current ACE Server configuration data. After entering the *`ace change`* command, you will be prompted for the configuration elements you want to change.

There is also an option to load the ACE configuration file. Use this option only if you have selected the alternate method of configuring the ACE Server on the system using the `sdconf.rec` file.

`ace reinit`
Allows you to reinitialize the system ACE client. This is required only if the server's IP address or encryption method has been changed. A reinitialization removes the user-named services file as described in the ACE Server documentation.

ALTERNATE METHOD OF CONFIGURATION

There is an alternate method of configuring the ACE Server database using a file on the ACE Server itself. If you decide to use this alternate method, you would TFTP the file sdconf.rec to the system, placing it in the `\config` directory. You would then activate the "load" through CFGEDIT (screen on page 220, selection 4) or through MANAGE MODE, using the *`ace change`* command. A restart would also activate the "load." After downloading the file, you will still need to specify the source IP address.

For more information on the `sdconf.rec` file and this alternate method of configuration, refer to the ACE Server documentation.

ACE AUTHENTICATION SERVER CONFIGURATION ELEMENTS

IP ADDRESS
The IP address in dotted decimal notation for the ACE Server. The IP address must match the address used for the server in its host machine's `\etc\hosts` file.

UDP PORT NUMBER
The UDP port number used by the ACE Server. The default value is 1024. This port number must match the port listed for the SecurID service in the host machine's `\etc\services` file.

NUMBER OF ACCESS REQUEST RETRIES
The number of Access Request Retries that the system will send to the ACE Server. The initial default value is 3. The acceptable range is from 0 to 32,767.

TIME BETWEEN ACCESS REQUEST RETRIES
The time between Access Request Retries sent from the system. The initial default value is 1 second. The acceptable range is from 1 to 10,000.

ENCRYPTION METHOD
This option should always indicate SDI, and is not currently configurable. If the ACE Server is not also configured to use SDI encryption, then any authentication attempts via the system will fail.

SOURCE IP ADDRESS
The source IP address for the ACE client should be a valid address (in dotted decimal notation) for the system. This address must match the IP address listed for the system in the ACE Server host machine's `/etc/hosts` file.

ACE AUTHENTICATION SERVER BACKGROUND INFORMATION

Access Control Encryption (ACE) is a database supported by the system. ACE operates using two components: client code and server code. The ACE Server software is installed on a UNIX-based system connected to the network. The client protocols allow the CyberSWITCH to communicate with the ACE Server, ultimately authenticating users.

CONFIGURING NETWORK LOGIN INFORMATION

OVERVIEW

The CyberSWITCH offers a number of configurable options to control the login process for this system and for off-node authentication servers. These options include:

- general network login configuration
- network login banners
- login configuration specific to RADIUS
- login configuration specific to TACACS

NETWORK LOGIN GENERAL CONFIGURATION

CONFIGURING GENERAL NETWORK LOGIN INFORMATION

USING CFGEDIT

1. Select *Security* from the main menu.

2. Select option (6), *Network Login Information* from the Security Menu. The following screen is displayed:

```
Network Login Information Menu:

   1) Network Login General Configuration
   2) Network Login Banners
   3) Login configuration Specific to RADIUS Server
   4) Login Configuration Specific to TACACS Server

Select function from above or <RET> for previous menu: 1
```

3. To customize general login prompts, choose selection (1) from the Network Login Information. The following menu is displayed:

```
Device Network Login General Configuration Menu:

   1)  Login Prompt                  is "Login ID: "
   2)  Dynamic Password Prompt       is "Dynamic Password: "
   3)  Passcode Prompt               is "Enter PASSCODE: "
   4)  Device Password Prompt        is "Password: "
   5)  Old Password Prompt           is "OLD Password: "
   6)  New Password Prompt           is "NEW Password: "
   7)  Login Attempts                is 3
   8)  Password Change Attempts      is 3
   9)  Authentication Timeout        is 30 seconds
   10) BOOTP Before Authentication   is Disabled
   11) Terminal Server Security      is Use Administrative Login

Select function from above or <RET> for previous menu:
```

By selecting items (1) through (6), you may change the wording of the specified prompts. Items (7) and (8) allow you to change the number of attempts for login or password change. Item (9) allows you to specify the amount of time before an *authentication timeout*. Enabling Item (10) allows BOOTP / DHCP to transmit an IP address to the user, so that the user may establish a

Telnet session for authentication. Item (11), *Terminal Server Security*, allows you to specify type of security for this special connection. See following description.

AUTHENTICATION TIMEOUT

Note: If using the Security Dynamics Ace Server, modify the timeout value to be greater than the change frequency value of the SecurID cards. Refer to the Security Dynamics documentation for more information on this change frequency value. In addition, if you are using Connection Services Manager (CSM) for call control management, this timeout value must represent the amount of time for the authenticating agent to respond to the login attempt, and for CSM to respond as well. These times should be based on network configuration.

TERMINAL SERVER SECURITY

To specify the type of security for terminal server connections, select *Terminal Server Security* from the *User Network Login General Configuration Menu*. A menu similar to the following will be displayed:

```
Terminal Server Security Menu:

Authentication Database Location:                    Status
               1)  RADIUS Authentication Server      NOT AVAILABLE
               2)  TACACS Authentication Server      AVAILABLE
               3)  ACE Authentication Server         NOT AVAILABLE
               4)  Use Administrative Login          AVAILABLE
               5)  Do not allow terminal access      AVAILABLE

Current Terminal Server Security is:  Use Administrative Login

Select function from above or <RET> for previous menu:
```

Select the type of authentication desired.

USING MANAGE MODE

`netlogin`

Displays the current network login configuration data. After entering the *`netlogin`* command, you will be prompted for the type of login configuration information you want. The prompt will resemble the CFGEDIT screen in which this information was originally configured. You may display: user level security general configuration, login banners, login configuration specific to RADIUS, and login configuration specific to TACACS.

`netlogin change`

Allows you to change the current network login configuration data. After entering the *`netlogin change`* command, you will be prompted for the type of login configuration information you want to change. The prompt will resemble the CFGEDIT screen in which this information was originally configured. You may change: user level security general configuration, login banners, login configuration specific to RADIUS, and login configuration specific to TACACS.

NETWORK LOGIN GENERAL CONFIGURATION BACKGROUND INFORMATION

Allows you to change the network login prompts. These include the prompts for:

- login ID
- dynamic password
- user password
- old password, new password
- passcode

You may also specify the number of login attempts, password change attempts and the amount of time in seconds before an authentication timeout.

Note: When using DHCP to provide temporary IP addresses to remote clients, it is important to enable BOOTP before Authentication if user authentication is used.

NETWORK LOGIN BANNERS

CONFIGURING NETWORK LOGIN BANNERS

USING CFGEDIT

1. Select option (2), *Network Login Banners* from the Network Login Information menu. If you need guidance to find this menu, refer to the instructions provided in the *Network Login General Configuration* configuration section. The following screen will be displayed:

```
Device Network Login Banner Menu:

The file "\CONFIG\Welcome.NEI" contains the Login Banner.
The file "\CONFIG\Motd.NEI" contains the Message of the Day.

   1) Login Banner                is "Login Please".
   2) Change Password Banner      is "Change Password".
   3) Login Successful Banner     is "**** Access Validated ****".
   4) Login Unsuccessful Banner   is "**** Access Denied ****".
   5) Call Control Failure Banner is "*CSM Denied Access*"

Select function from above or <RET> for previous menu:
```

Note the following: the `Welcome.NEI` file and the `Motd.NEI` file are user-created files. The `Welcome.NEI` file contains text to be displayed prior to system login. It precedes the actual login banner. If no `Welcome.NEI` file exists, the login banner alone is displayed. The `Motd.NEI` file (Message-of-the-Day file) is displayed after successful login. Like the Welcome.NEI file, the `Motd.NEI` file is optional.

USING MANAGE MODE

`netlogin`

Displays the current network login configuration data. After entering the *`netlogin`* command, you will be prompted for the type of login configuration information you want. The prompt will resemble the CFGEDIT screen in which this information was originally configured. You may display: user level security general configuration, login banners, login configuration specific to RADIUS, and login configuration specific to TACACS.

netlogin change

Allows you to change the current network login configuration data. After entering the *netlogin change* command, you will be prompted for the type of login configuration information you want to change. The prompt will resemble the CFGEDIT screen in which this information was originally configured. You may change: user level security general configuration, login banners, login configuration specific to RADIUS, and login configuration specific to TACACS.

NETWORK LOGIN BANNERS BACKGROUND INFORMATION

Allows you to customize the various system banners: login, change password, login successful and login unsuccessful. You may also define a "Welcome" banner and a "Message-of-the-Day" banner. You do so by creating a `welcome.nei` file and a `motd.nei` file on the system's `\config` directory. (Refer to the *Software Overview* chapter for file information). The creation of these files is optional.

LOGIN CONFIGURATION SPECIFIC TO RADIUS SERVER

CONFIGURING RADIUS SERVER LOGIN INFORMATION

USING CFGEDIT

1. Select option (3), *Login Configuration Specific to RADIUS Server* from the Network Login Information menu. If you need guidance to find this menu, refer to the instructions provided in the *Network Login General Configuration* configuration section. The following screen will be displayed:

```
RADIUS Specific Device Login Menu:

   1) Change Password Control Character is DISABLED.
   2) Prompt Order for Device Login.

Select function from above or <RET> for previous menu: 1
```

2. Selection (1) from the RADIUS Specific Device Login Menu allows you to change the password control character:

```
Enter control character used to switch from LOGIN to CHANGE PASSWORD mode.
Select the control character that you wish to us by typing
caret ('^') followed by another character (example: ^A),
or '0' to disable [Default = DISABLED]? <RET>
```

3. Selection (2) from the RADIUS Specific Device Login Menu allows you to customize the prompt order for device login. This prompt is particularly important, because the order of prompts must be the same as the order expected by the RADIUS server. Selection (2) displays the following:

```
RADIUS Device Login Prompt Order Menu:

Current Prompt Order is:
-----------------------------------------------------------------
    First Prompt     is LOGIN ID PROMPT (fixed)
    Second Prompt    is USER PASSWORD PROMPT


   1) Prompt Order

Select function from above or <RET> for previous menu: 1
```

```
Prompts available for Second Prompt

   1) USER PASSWORD
   2) DYNAMIC PASSWORD

Select function from above or <RET> for previous menu:
```

USING MANAGE MODE

netlogin

Displays the current network login configuration data. After entering the *netlogin* command, you will be prompted for the type of login configuration information you want. The prompt will resemble the CFGEDIT screen in which this information was originally configured. You may display: user level security general configuration, login banners, login configuration specific to RADIUS, and login configuration specific to TACACS.

netlogin change

Allows you to change the current network login configuration data. After entering the *netlogin change* command, you will be prompted for the type of login configuration information you want to change. The prompt will resemble the CFGEDIT screen in which this information was originally configured. You may change: user level security general configuration, login banners, login configuration specific to RADIUS, and login configuration specific to TACACS.

LOGIN CONFIGURATION SPECIFIC TO RADIUS SERVER BACKGROUND INFORMATION

Login configuration parameters specific to RADIUS include the specification of prompt order and a password control character.

The prompt order specified on the system must match the prompt order specified on the RADIUS server. The default order is:

- First prompt: LOGIN ID PROMPT (fixed)
- Second prompt: DYNAMIC PASSWORD PROMPT
- Third prompt: USER PASSWORD PROMPT

If you need to change this order, you may specify this order of prompts in the login process.

The password control character is a key sequence you specify to switch between the login mode and the change password mode. In order to enable this feature for the general user, you need to configure this password control character.

LOGIN CONFIGURATION SPECIFIC TO TACACS SERVER

CONFIGURING TACACS SERVER LOGIN INFORMATION

USING CFGEDIT

1. Select option (4), *Login Configuration Specific to TACACS Server* from the Network Login Information menu. If you need guidance to find this menu, refer to the instructions provided in the *Network Login General Configuration* configuration section. The following screen will be displayed:

```
TACACS Specific Device Login Menu:

   1) Password Control Character is ^R.
   2) Prompt Order for Device Login.
   3) Messages for TACACS Return Codes.
   4) Return to the Previous Menu.

Select function from above or <RET> for previous menu: 1
```

2. Selection (1) from the TACACS Specific Device Login Menu allows you to change the password control character:

```
Enter control character used to switch from LOGIN to CHANGE PASSWORD mode.
Select the control character that you wish to us by typing
caret ('^') followed by another character (example: ^A),
or '0' to disable [Default = ^R]? <RET>
```

3. Selection (2) from the TACACS Specific Device Login Menu allows you to customize the prompt order for device login. This prompt is particularly important, because the order of prompts must be the same as the order expected by the TACACS server. Selection (2) displays the following:

```
TACACS Device Login Prompt Order Menu:

Current Prompt Order is:
-----------------------------------------------------------------
    First Prompt     is LOGIN ID PROMPT (fixed)
    Second Prompt    is DYNAMIC PASSWORD PROMPT
    Third Prompt     is USER PASSWORD PROMPT


   1) Prompt Order

Select function from above or <RET> for previous menu:
```

4. Selection (3) from the TACACS Specific Device Login Menu allows you to adjust the return code messages upon login attempt:

```
TACACS Return Code Messages Menu:

      RESPONSE    REASON      MESSAGE
    ------------------------------------------------------------------
   1) ACCEPTED(1) NONE(0)     ""
   2) ACCEPTED(1) EXPIRING(1) "**** Password about to expire ****"
   3) ACCEPTED(1) PASSWORD(2) "**** Password expiration imminent ****"
   4) REJECTED(2) NONE(0)     "**** Login invalid ****"
   5) REJECTED(2) EXPIRING(1) "**** Please change PIN ****"
   6) REJECTED(2) PASSWORD(2) "**** Device/Password invalid ****"
   7) REJECTED(2) DENIED(3)   ""

Select function from above or <RET> for previous menu:
```

Note: There is no customization of Specific Device Login for the ACE Server.

USING MANAGE MODE

`netlogin`

Displays the current network login configuration data. After entering the *`netlogin`* command, you will be prompted for the type of login configuration information you want. The prompt will resemble the CFGEDIT screen in which this information was originally configured. You may display: user level security general configuration, login banners, login configuration specific to RADIUS, and login configuration specific to TACACS.

`netlogin change`

Allows you to change the current network login configuration data. After entering the *`netlogin change`* command, you will be prompted for the type of login configuration information you want to change. The prompt will resemble the CFGEDIT screen in which this information was originally configured. You may change: user level security general configuration, login banners, login configuration specific to RADIUS, and login configuration specific to TACACS.

LOGIN CONFIGURATION SPECIFIC TO TACACS SERVER BACKGROUND INFORMATION

LOGIN ELEMENTS SPECIFIC TO TACACS

There are login configuration parameters specific to TACACS. These include the specification of prompt order, a password control character, and specification of messages for TACACS return codes.

The prompt order specified on the system must match the prompt order specified on the TACACS server. The default order is:
First prompt: LOGIN ID PROMPT (fixed)
Second prompt: DYNAMIC PASSWORD PROMPT
Third prompt: USER PASSWORD PROMPT

If you need to change this order, you may specify this order of prompts in the login process.

The password control character is a key sequence you specify to switch between the login mode and the change password mode. In order to enable this feature for the general user, you need to configure this password control character.

TACACS may provide return code messages upon user login. You may customize these messages through CFGEDIT. The default messages are as follows:

If the login process was successful, but the user password is about to expire, one of the following messages is displayed:

- Password about to expire
- Password expiration imminent

If the login process is unsuccessful, one of the following messages is displayed:

- Login invalid
- Please change PIN
- User/Password invalid

CONFIGURING ENCRYPTION

OVERVIEW

The CyberSWITCH encryption option provides 56-bit data encryption through two different implementations:

- IP (or Network Layer) Security
- PPP (or Link Layer) Encryption

These implementations use the Data Encryption Standard (DES) algorithm. DES provides data security for transmissions over the WAN between encryption devices, either through PPP or frame relay connections, or over unprotected media, such as the Internet.

If you have purchased the CyberSWITCH encryption option, you will need to properly configure the feature to make it operational. This involves configuring the following through CFGEDIT:

- An encryption adapter (through *Resources*)
- Security Associations and / or Authentication Headers (through *Options*). These are for IP security only.
- Link Layer Encryption parameters (through *Security*). These are for PPP Encryption only.

Note: If you have an existing CyberSWITCH without encryption, you may upgrade to an encrypted system. To do this, you must install the proper adapter and encryption-capable software, then configure the encryption parameters. However, take note that this is a one-way process! (You *cannot* "downgrade" an encryption-capable system to a non-encryption software release).

If CyberSWITCH encryption is new to you, we suggest you review the *Background Information* and *Configuration Elements* sections before attempting configuration. Then continue with the following configuration process.

CONFIGURATION

CONFIGURING AN ENCRYPTION ADAPTER

USING CFGEDIT

1. From the CFGEDIT Main Menu, select *Physical Resources*.
2. Select *Resource*.
3. Select *Add a Resource*.
4. From the list of resource types, choose *DES_RSA*.
5. Identify the slot number containing the added encryption adapter.

Note: Only one encryption adapter is allowed per system.

USING MANAGE MODE

You may not add an encryption adapter via Manage Mode.

CONFIGURING SECURITY ASSOCIATIONS AND AUTHENTICATION (IP SECURITY ONLY)

IP Security encryption configuration consists of the following elements:

- setting up security associations for Encapsulating Security Payload (ESP)
- optionally specifying keys for Authentication Headers (AH)

Security Associations are necessary for IP networks that plan to use an untrusted / unprotected media, such as the Internet. Security Associations identify the IP addresses for which exchanged datagrams must be encrypted. They also provide the parameters necessary to encrypt and decrypt IP datagrams. By default, the CyberSWITCH has no Security Associations. Therefore, to enable encryption, you must specify these associations.

When configuring two CyberSWITCH nodes, the security association information from one node must parallel the information on the other node. The parameters for *Transform Menu*, *Shared Secret Key*, and *Security Parameter Index* must be the same on both nodes in order for the nodes to communicate.

Likewise, if you plan to authenticate packets prior to encryption / decryption, the authentication key information from one node must parallel the information on the other node.

USING CFGEDIT

1. From the CFGEDIT Main Menu, select *Options*.
2. Select *IP Routing*. If IP routing is disabled, enable this now.
3. Select *IP Security Associations*.
4. Select *Add*. Respond to the following series of questions:

```
Security Association Packet Direction Menu:

   1) Outgoing (packets from trusted local subnet to remote site)
   2) Incoming (packets to trusted local subnet from remote site)
   3) Both outgoing and incoming

ID of the Direction for this Security Association [default = 3] ?
```

```
Enter the Final Destination IP address in dotted decimal notation or <RET> to cancel?
197.1.0.0

Enter the number of significant bits for the Subnet Mask   [default = 8 ]?  16

Enter the Source IP Address in dotted decimal notation or <RET> to cancel?   197.4.0.0

Enter the number of significant bits for the Subnet Mask  [default = 8]?   16

Enter the Destination Gateway/Router IP Address in dotted decimal notation or <RET>
to cancel?   197.1.1.1

Security Association IV Length Menu:
   1) 32 bits
   2) 64 bits

ID of IV length to use:  [default = 2]?

Enter the Shared Secret Encryption Key for this Security Association:
AAABBB1234567890
```

Note: For the *Final Destination* and *Source* IP addresses, you may enter the entire address (i.e., 197.1.2.2 vs. 197.1.0.0); however, the subnet mask will determine how many significant bits the system will actually consider.

5. The next series of questions pertain to the Authentication Header. To implement an Authentication Header, select *Authentication using MD5*, and provide a shared secret authentication key. If you do not wish to use an Authentication Header, select *No Authentication*:

```
Security Association Authentication Menu:

   1) No Authentication
   2) Authentication using MD5
   3) Id of Authentication to use [default = 1]?  2

Enter the Shared Secret Authentication Key for this Association:
```

6. Complete this IP Security configuration:

```
Enter the Security Parameter Index (SPI) for this Security Association: 12345678

Select function from above or <RET> for previous menu:
```

Refer to the Background Information section for a pertinent example of *IP Encryption* configuration.

USING MANAGE MODE

Not currently supported.

CONFIGURING LINK LAYER ENCRYPTION (PPP ENCRYPTION ONLY)

Link Layer Encryption provides encryption capabilities *for all protocols* within a PPP environment. This feature allows you to:

- enable encryption for PPP devices,
- select either an automatic key exchange or manually-configured keys, and then
- for manual-key configuration, assign key values to devices to encrypt/decrypt datagrams

USING CFGEDIT

1. From the CFGEDIT Main Menu, select *Security*.
2. Select *Device Level Databases.*
3. Select *On-node device entries.*
4. Follow on-screen instructions to enable device level security, and then add a new (or change an existing) device. Refer to *Configuring Device Level Databases* for details.
5. From the Device Table Menu, select *Encryption*. A menu similar to the following will be displayed:

```
Device PPP Encryption Menu

   1) Decryption/Encryption          DISABLED
   2) Proprietary Key Exchange       DISABLED
   3) Decryption key
   4) Encryption key

Id of parameter to change or <RET> to cancel:
```

7. Enable the *Decryption/Encryption* feature. (This selection is a toggle switch).
8. Configure encryption key implementation:
   - If you plan to use the CyberSWITCH's automated key exchange, enable *Proprietary Key Exchange*. (This selection is a toggle switch.) Then skip to step 11.
   - If you plan to use manually-configured keys, verify that *Proprietary Key Exchange* is disabled, and continue with step 9.
9. Specify an 8-byte (16-hex digits) *decryption key*. This value is an arbitrary value; however, it must be the *same as the encryption key* on the other side of the connection.
10. Specify an 8-byte (16-hex digits) *encryption key*. This value is an arbitrary value; however, it must be the *same as the decryption key* on the other side of the connection.
11. Press<RET> to return to the Device Table Menu.

Note: You may use the same value for both your encryption and decryption keys at a single site. However, we recommend different values for these keys to provide the utmost security.

Refer to the Background Information section for a pertinent example of *Link Layer Encryption.*

USING MANAGE MODE

Not supported.

ENCRYPTION CONFIGURATION ELEMENTS

RESOURCE TYPE

The type of adapter (resource) that plugs into the system. In this specific case, you need to specify the DES/RSA encryption adapter. This adapter is available to U.S. and Canadian markets only. Export or use in other countries requires appropriate permission from the U.S. Government.

The DES/RSA adapter implements the Data Encryption Standard algorithm for encryption purposes, and also includes an RSA chip. (Refer to the *System Adapters* appendix for adapter illustrations.)

RESOURCE SLOT

The slot number in the CyberSWITCH into which the resource is plugged. (Do not use slot 1).

The following elements apply to *Network Layer Encryption* only:

SECURITY ASSOCIATION PACKET DIRECTION

Specifies whether the security associations refer to outgoing packets, incoming packets, or both. The default is both. For utmost security, you may want to consider configuring separate security

associations for incoming and outgoing packets. The incoming packet security association on site "A" must match the outgoing packet security association on site "B" and vice versa.

FINAL DESTINATION IP ADDRESS
IP address using dotted decimal notation that specifies the remote ("destination") trusted network or host.

SUBNET MASK
The subnet mask identifies a subnetwork. The value of the mask determines which part of the 32-bit IP address is the "network" address. For example, if you have an IP address of 197.4.2.2 and specify a 16-bit mask, the system recognizes the subnetwork as 197.4.0.0. The last two bytes (i.e., the last 16 bits) of the IP address are ignored.

The Subnet mask is specified by entering the number of contiguous bits that are set for the mask. The mask bits start at the most significant bit of the IP address field and proceed to the least significant bit. A subnet mask of 255.255.255.255 equals 32 bits; a subnet mask of 255.255.255.0 equals 24 bits, and so on.

GATEWAY/ROUTER IP ADDRESS
IP address using dotted decimal notation that provides access to (i.e., encryption and decryption for) the remote trusted (sub-) network or host. The IP address of the gateway must be on the (sub) network connected to a defined interface.

SOURCE IP ADDRESS
IP address using dotted decimal notation that specifies the local ("source") trusted network or host.

SECURITY ASSOCIATION IV LENGTH MENU
The IV or Initial Value Length refers to the number of bits to be added to a soon-to-be encrypted datagram in order to make proper encryption calculations. Your choices are 32 bits or 64 bits; 64 is the default.

SHARED SECRET ENCRYPTION KEY (IP NETWORK ENCRYPTION)
The shared secret key must be 64 bits (16 hexadecimal digits) in length. You must configure the same shared secret on each CyberSWITCH node sharing this security association.

As opposed to a password, a shared secret is not sent across lines, and therefore is not susceptible to interception. The shared secret is used to encrypt or decrypt data.

SECURITY ASSOCIATION AUTHENTICATION MENU (IP NETWORK ENCRYPTION)
This menu specifies whether or not to use an Authentication Header in addition to ESP encryption. Choices are: *No Authentication* or *Authentication using MD5.*

AUTHENTICATION USING MD5 (IP NETWORK ENCRYPTION)
Specifies Authentication Header (AH) implementation using the Message Digest 5 (MD5) algorithm with 128-bit keys. AH can be enabled (with appropriate shared secret keys) for each individual security association.

SHARED SECRET AUTHENTICATION KEY (IP NETWORK ENCRYPTION)
The shared secret key must be 128 bits (32 hexadecimal digits) in length. You must configure the same shared secret on each CyberSWITCH node sharing in authentication implementation.

SECURITY PARAMETER INDEX (SPI)
A 32-bit number (eight hexadecimal digits) used to identify the security associations between CyberSWITCH nodes. The SPI must be greater than or equal to 00000100hex. The SPI is transmitted in the Encapsulating Security Payload (ESP) header and used by the peer CyberSWITCH node to identify the necessary information to decrypt the ESP payload.

The following element applies to *Link Layer Encryption* only:

PROPRIETARY KEY EXCHANGE
When using Link Layer encryption, this feature supports an automated key exchange (for Cabletron products only). If you enable this feature, you do not need to manually specify encryption / decryption keys.

ENCRYPTION / DECRYPTION KEY
This key is used for PPP devices only, and must be 16 digits in length. You may use any combination of hexadecimal digits in the key. The encryption key you configure on one side of the connection (site "A") must match the decryption key you configure on the other side of the connection (site "B").

ENCRYPTION BACKGROUND INFORMATION

IP NETWORK LAYER ENCRYPTION

IP Network Layer Encryption consists of:
- an Encapsulating Security Payload (ESP) implementation
- Authentication Headers (AH)

The CyberSWITCH provides IP Security by using either ESP or AH, or a combination of the two.

ESP IMPLEMENTATION

The IP Encryption feature provides a connection between two or more trusted subnets through the Internet or any other IP network. IP datagrams transmitted from one trusted subnet to another trusted subnet funnel through a CyberSWITCH node where they are encrypted and encapsulated. The destination address on the encapsulated datagram is that of the CyberSWITCH node servicing the other trusted subnet.

IP datagrams to these IP destination addresses are encrypted and encapsulated with an Encapsulating Security Payload (ESP) header. The ESP header indicates a destination address of an intermediate CyberSWITCH node which is responsible for decrypting and decapsulating these packets before sending them on to their intended destination.

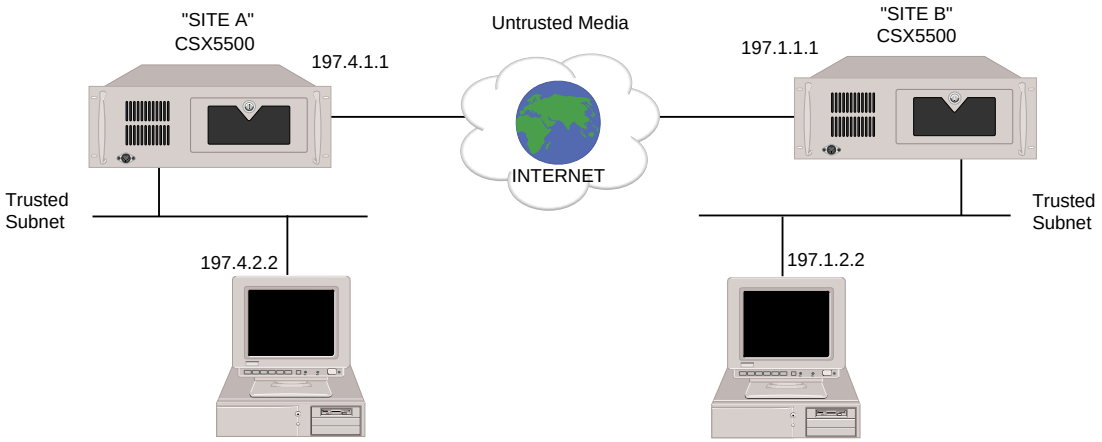
When the IP datagram reaches the destination CyberSWITCH node, the ESP header is removed, the ESP payload is decrypted, and the original IP datagram is forwarded to its original destination.

The CyberSWITCH requires Security Associations to identify:
- range of IP addresses (i.e., one for source subnet and one for destination subnet)
- encryption parameters to be used to encrypt communications to those IP addresses
- IP address of the peer CyberSWITCH responsible for decrypting the communications

The peer must also have corresponding Security Associations. (Note that the gateway address and the source / destination subnet addresses are switched to reflect the *peer* subnet.)

Security Associations between peer CyberSWITCH nodes are identified by a Security Parameter Index (SPI). The SPI is transmitted in the ESP header and is used by the peer node to identify the necessary information to decrypt the ESP payload.

IP ENCRYPTION EXAMPLE



Site "A"	Security Associations	
	Outgoing:	*Incoming:*
Final Destination:	197.1.2.2	197.4.2.2
Mask:	16 bits	16 bits
Destination gateway:	197.1.1.1	197.1.1.1
Shared Secret Key:	AAABBB1234567890	9876543210ABCDEF
SPI:	12345678	8888CCCC

Site "B"	Security Associations	
	Outgoing:	*Incoming:*
Final Destination:	197.4.2.2	197.1.2.2
Mask:	16 bits	16 bits
Destination gateway:	197.4.1.1	197.4.1.1
Shared Secret Key:	9876543210ABCDEF	AAABBB1234567890
SPI:	8888CCCC	12345678

AUTHENTICATION HEADERS

Authentication Header (AH) protocol provides integrity and authentication for IP datagrams by assuring that a received packet originated from the destination it claims. Packets originating from the CyberSWITCH may be authenticated with AH protocol, as long as AH is enabled and properly configured.

On the CyberSWITCH, AH is added to a packet after ESP application. When a remote node receives the encrypted packet, it first processes the authentication information in the AH. If the AH information is valid, the node proceeds to decrypt the packet. If authentication fails, the packet is dropped.

LINK LAYER ENCRYPTION

Link layer encryption is available for WAN services using PPP (data-link layer) protocol. It accommodates network layer protocols such as IP, IPX and AppleTalk protocols, and can also be used for bridged data. Link layer encryption may use the DES algorithm along with configured encryption keys, or it may use an automated key exchange. Link layer encryption (using either the manual keys or the automated key exchange) is set up on a per-device basis. Device-level authentication is required when using Link Layer encryption.

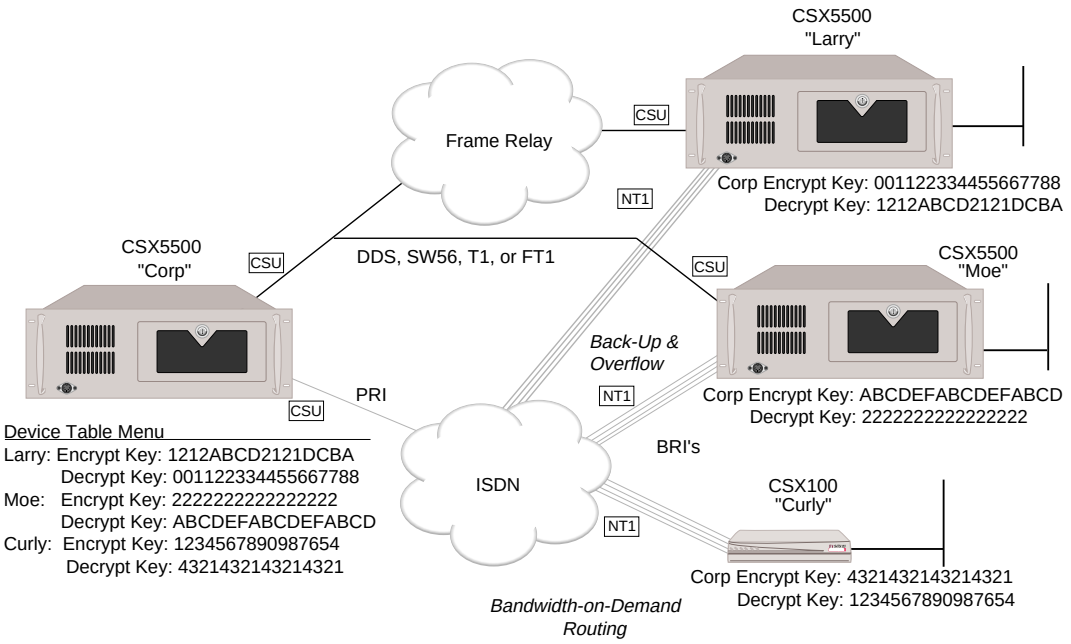
LINK LAYER ENCRYPTION: MANUALLY-CONFIGURED KEYS

When using manually-configured keys, each device needs to have two keys - one for encrypting outgoing data, and one for decrypting incoming data. These manually-configured keys need to match the keys configured on the remote node. That is, the CyberSWITCH's encryption key needs to match the remote node's decryption key, and vice versa.

The following graphic illustrates a CyberSWITCH encryption network using manually-configured keys. The nodes are communicating via Point-to-Point Protocol over various types of WAN links:

- dedicated lines
- ISDN
- Frame Relay

The CyberSWITCH will provide privacy for all communications across each of the WAN links by encrypting data using DES. Communications on the LAN will be in the clear.



AUTOMATED KEY EXCHANGE

The CyberSWITCH's automated key exchange uses a proprietary protocol defined for use with Cabletron remote access products. This proprietary protocol exchanges information during ECP (Encryption Control Protocol) negotiation to produce proper keys.

To use automated key exchange, the feature must be enabled for each device, and the DES/RSA resource must be properly configured and installed on the CyberSWITCH.

When a PPP call to a particular device is initiated or received, the CyberSWITCH will attempt to use ECP to negotiate encryption (if it is enabled for this device). If ECP negotiation succeeds, then data transmitted over the PPP link will be encrypted using 56-bit session keys. The CyberSWITCH will encrypt outgoing plain text using the encryption key, and decrypt incoming enciphered data using the decryption key. If ECP negotiation fails, then the CyberSWITCH will bring down the call. When encryption is enabled, an unsecure PPP session will not be allowed.

INTERACTION WITH OTHER FEATURES

IP FILTERS

You can use IP Filters to automatically discard or forward IP datagrams based on the contents of various fields within the IP datagram. You can also use *ESP Tunnel Mode* to allow IP datagrams to tunnel through IP filters. To assure the proper filtering, you must understand whether an IP filter is applied to the encapsulated datagram or the unencapsulated datagram.

When an ESP datagram is simply passing through a node to be routed from a previous hop to the next hop, any IP filters will be applied only to the encapsulated datagram. The original source and destination, protocol, and any other information from the original datagram will not be used in any filtering logic.

On the source gateway, the original datagram will tunnel through any output filters. However, on the destination gateway, input filters will be applied first to the ESP and then to the original datagram. The ESP datagram will be filtered by an output filter on the source gateway and an input filter on the destination gateway. Global filters on both gateways apply to both the ESP and the original datagram.

The following tables list which filters are applicable to the different datagrams:

Original Datagram	Input filters	Global filters	Output filters
source gateway	no	yes	no
intermediate node	no	no	no
destination gateway	yes	yes	no

ESP Datagram	Input filters	Global filters	Output filters
source gateway	no	yes	yes
intermediate node	yes	yes	yes
destination gateway	yes	yes	no

MULTIPLE MAC/IP ADDRESSES

For backup purposes, you may want to consider using the multiple MAC or *multiple IP address* feature to set up redundant configurations to use in conjunction with encryption. In such configurations, you must be sure that all CyberSWITCH nodes have the same or comparable Security Associations. When multiple paths through different secure gateways exist, you must be sure such paths are properly protected.

PPP COMPRESSION

For IP Layer encryption:
We do not recommend using PPP compression if you anticipate a large percentage of encrypted traffic across your network. PPP protocol runs at a lower layer than Internet Protocol; therefore, any data compression performed on ESP datagrams is attempted *after* the packet has been encrypted. Unfortunately, well-encrypted data is not compressible.

For Link Layer encryption:
PPP compression is available. This compression takes place before the actual encryption.

ADVANCED CONFIGURATION

We define advanced configuration as the configuration you may use to fine tune your system, or to configure options that are not necessarily needed by the majority of users. For example, to configure an alternate access (an alternate to ISDN access), this would be considered advanced configuration.

We include the following chapters in the *Advanced Configuration* segment of the *User's Guide*:

- *Configuring Alternate Accesses*
  An access defines the connection details the CyberSWITCH uses to reach the network. The default access is ISDN access, a switched-network access. This chapter provides instructions for configuring the non-default types of accesses.

- *Configuring Advanced Bridging*
  Instructions for configuring the following advanced bridging options: bridge dial out, Spanning Tree Protocol, mode of operation, and bridging filters.

- *Configuring Advanced IP Routing*
  Instructions for configuring the following advanced IP routing options: static ARP table entries, enable / disable isolated mode, static routes lookup, IP address pool, and DHCP.

- *Configuring IPX*
  Instructions for configuring the IPX feature.

- *Configuring AppleTalk Routing*
  Instructions for configuring the AppleTalk Routing feature.

- *Configuring SNMP*
  Instructions for configuring SNMP capabilities.

- *Configuring Call Control*
  Instructions for configuring the options that control how the system will make and accept calls.

- *Configuring Other Advanced Options*
  Instructions for configuring advanced system options that are not covered in the previous chapters. Information is included for the following advanced options: digital modem, PPP, default line protocol, log options, system compression options, TFTP, and file attributes.

CONFIGURING ALTERNATE ACCESSES

OVERVIEW

An access defines the connection details the CyberSWITCH uses to reach the network. The default access is ISDN access, a switched-network access. Configurable accesses are required for *dedicated network connections*, and for packet-switched network connections including *X.25* and *frame relay connections*. Refer to the following information for the alternate access you wish to add.

DEDICATED ACCESSES

CONFIGURING A DEDICATED ACCESS

USING CFGEDIT

1. Select *Access* from the Physical Resources menu, then follow the onscreen instructions to add a dedicated access.

2. Select the line Id of the line you will use for this access.

3. For BRI and PRI lines: select the bearer channels the access will use.

4. For V.35 or RS232 resources, select the clocking type (internal or external clocking).

5. For Internal clocking, select the access' data rate.

6. For External clocking, enter the Data Rate in bits per second.

7. Select the line protocol. In almost all cases, select PPP. Select HDLC only if you are connecting to a device that uses HDLC over a dedicated access.

8. Enter the device name tied to this access (optional for accesses using PPP protocol, mandatory for accesses using HDLC protocol).

Note: Device authentication must be enabled for dedicated accesses to properly identify the remote device and provide switched backup and overflow to that device. Remote devices using a dedicated connection must use PPP for device authentication. Authentication configuration is described in *Security Configuration*.

USING MANAGE MODE COMMANDS

dedacc
Displays previously configured dedicated accesses.

DEDICATED ACCESS CONFIGURATION ELEMENTS

LINES

The line that will be used for the dedicated access. A dedicated access can be defined on either a BRI, a PRI, a network V.35, or a network RS232 line.

BEARER CHANNELS

For BRI and PRI lines only. Also referred to as B channels. B channels can carry voice or data in either direction.

CLOCKING TYPE

For V.35 and RS232 lines only. Clocking types can be either external or internal. Dedicated connections usually use external clocking.

LINE PROTOCOL

Designates the type of line protocol that will be used on the dedicated connection. PPP line protocol is the correct selection for most configurations. HDLC protocol may work for devices that only support HDLC protocol.

DEVICE NAME (OPTIONAL)

Optional parameter. The device name of the device assigned to this dedicated connection. The device name may be up to 17 characters in length, and is case sensitive. If you configure this parameter, and, in addition, turn off outbound authentication for this device, no authentication will be needed for this particular device. If you do not configure this parameter, device authorization is required for the device.

DEDICATED ACCESS BACKGROUND INFORMATION

To access dedicated network connections, there must be a physical connection between the network and the CyberSWITCH. The dedicated access defines how the CyberSWITCH will use this physical connection.

The dedicated connection is used in addition to any switched connections that can be made to provide overflow data capacity to the remote device. The dedicated connection is brought up at initialization time. The Throughput Monitor starts monitoring the dedicated connection for an overload condition. When link utilization causes an overload condition, additional switched connections will be made to the remote device based on the data rate configured for that device. When the link utilization causes an underload condition, the switched connections will be released with the dedicated connection remaining active.

Switched connections can also be used to provide backup connectivity to the remote device in case the dedicated connection fails. If the dedicated connection goes down, and there is network traffic, switched connections will be made to the remote device based on the data rate configured for that device thus providing backup for the dedicated connection. When the dedicated connection comes back up, it will be aggregated together with any switched connections that may be active.

When the link utilization causes an underload condition, the switched connections will be released with the dedicated connection remaining active.

Device level authentication must be enabled for dedicated accesses to properly identify the remote device and provide switched backup and overflow to that device.

To define a Dedicated Access, you must select a previously defined line. Then, input the details required to use the line.

Notes: To achieve maximum bandwidth, you could theoretically dedicate two T1s to one remote device (3072 Kbps). Any configuration above this maximum bandwidth is not supported.

Keep in mind that you can aggregate a maximum of 32 connections. These connections can be any combination of dedicated and / or switched connections to the same device. For maximum performance, however, we recommend aggregating no more than eight connections at a time.

X.25 ACCESSES

CONFIGURING AN X.25 ACCESS

Note the following:

- X.25 accesses are available only if you have purchased the additional software module for packet switched accesses. X.25 is not available on CSX158 platforms.
- To establish virtual circuits over X.25, you must enable device level security (page 167).
- You may only configure one X.25 access per CyberSWITCH, and one line per access.
- Bearer channels used by X.25 accesses can not be shared by other access types.
- Compression is not available over X.25 connections.

USING CFGEDIT

To add an X.25 access, several categories of information must be configured, including basic configuration information including line information, Link Access Procedure Balanced (LAPB) parameters, X.25 parameters, and finally, virtual circuit parameters. A separate section for configuring each of the above categories follows.

Notes: If you are unsure of a value, select the default value if one is provided. If you want to change an existing X.25 access configuration, select the "change" option from the main X.25 Access menu. A submenu will display the various categories described below. You can then select to edit individual categories without paging through all of the parameters. It is important to note that the line used for an existing X.25 access cannot be changed. Individual characteristics of the line can change, for example, the data rate, bearers, or Public Packet Switched Network (PPSN) phone number. If another line is to be used, the existing access must be deleted, and added back in.

BASIC CONFIGURATION INFORMATION

1. Select *Access* from the Physical Resources menu, then follow the onscreen instructions to add an X.25 access.

2. Select the line Id this access will be using. A BRI line that is in use by another type of access will not be available for use by an X.25 access.

3. Enter an X.25 access name of 1 to 16 non-blank, alpha-numeric characters. The X.25 access name is a user-defined name and is provided as an aid in helping you track events occurring on an X.25 access.

4. Enter the X.121 address of the local DTE (the CyberSWITCH).
5. Select the data rate for the line.
6. Enter a list of bearers (a channel map). For PRI lines, the range of channels is from 1 to 24. For BRI lines, the range of channels is from 1 to 2. Separate bearer channels by commas, and / or list a range by using a dash (-).

LAPB CONFIGURATION INFORMATION

1. Enter the LAPB sequence number range to use, regular, or extended. Extended sequence numbering allows for frames to be assigned sequence numbers from 0-127 (modulo 128), as opposed to 0-7 (modulo 8).

2. Enter the duration of Timer T1, which is the maximum time to wait for responses to pending commands.

3. Enter the duration of Timer T3, which is used to signal that an excessively long idle time is occurring on the link. LAPB requires that Timer T3 be greater than Timer T1.

4. Enter the maximum number of frame re-transmissions that can be performed (this is commonly known as “N2”).

5. Enter the maximum number of frames that the transmitting station may have outstanding at any given time (this is commonly known as “K”). The range for this parameter will be 1-7 if the Modulo 8 sequence numbers are being used for LAPB, or 1-127 if Modulo 128 sequence numbers are being used.

X.25 CONFIGURATION INFORMATION

1. Configure the X.25 Logical Channel Assignments. This requires entering the maximum number of PVCs and SVCs to be supported. For X.25 over B-channel, a total of 48 virtual circuits are supported; over D-channel 8 virtual circuits are supported. Therefore, the total number of PVCs and SVCs combined cannot exceed the maximum number of VCs.
   a. Enter the maximum number of PVCs to support.
   b. Enter the maximum number of SVCs to support.

2. Configure the X.25 Timers.
   a. Enter the duration of Timer T20.
      This timer designates the time limit in which a restart confirmation must be returned by the DCE (the PPSN) after a restart request has been issued by the DTE (the CyberSWITCH).
   b. Enter the duration of Timer T21.
      This timer designates the time limit in which a call connected response must be returned by the DCE (the PPSN) after a call request has been issued by the DTE (the CyberSWITCH).
   c. Enter the duration of Timer T22.
      This timer designates the time limit in which a reset confirmation must be returned by the DCE (the PPSN) after a reset request has been issued by the DTE (the CyberSWITCH).
   d. Enter the duration of Timer T23.
      This timer designates the time limit in which a clear confirmation must be returned by the DCE (the PPSN) after a clear request has been issued by the DTE (the CyberSWITCH).

3. Configure the X.25 Reliability, Windows, and Acknowledgment Facilities.
   a. Select the type of sequence numbers to be used for X.25: regular or extended. Extended sequence numbering allows for packets to be assigned sequence numbers from 0-127 (modulo 128), as opposed to 0-7 (modulo 8).
   b. Enter the Maximum Window Size. This is the largest possible window size to be supported on any virtual circuit. SVCs that support window size negotiation will never allow the agreed upon window size to exceed this value. If regular (modulo 8) sequence numbers are being used, the range of possible window sizes is 1-7. If extended (modulo 128) sequence numbers are being used, the range of possible window sizes is 1-127.
   c. Select the Maximum Packet Size. This value is used to determine the maximum packet size that the system will support for X.25 connections. When packet size negotiation is performed on SVCs, this value will be used as the upper bound.

4. Configure the X.25 Quality-of-Service Facilities for SVCs.
   The first three items are configured for SVCs that can perform negotiation.
   a. Select the Maximum Throughput Class. This value is used to determine the maximum throughput class that the system will support for X.25 connections. When throughput class negotiation is performed on SVCs, this value will be used as the upper bound.
   b. Choose whether Flow Control Negotiation is to be supported for SVCs (negotiation is not performed on PVCs).
   c. Choose whether Throughput Class Negotiation is to be supported for SVCs (negotiation is not performed on PVCs).

   The next 6 items configured are the nonstandard default parameters for SVCs that do not support negotiation. These parameters are used on SVCs that do not use the standard X.25 values, but also do not support any facility negotiation.

   d. Enter the Nonstandard Default Transmit Window Size. The range of allowable values for this parameter is based upon configured sequence number modulus (1-7 for Modulo 8, and 1-127 for Modulo 128).
   e. Enter the Nonstandard Default Receive Window Size.
   f. Select the Nonstandard Default Transmit Packet Size.
   g. Select the Nonstandard Default Receive Packet Size.
   h. Select the Nonstandard Default Transmit Throughput Class.
   i. Select the Nonstandard Default Receive Throughput Class.

5. Configure the X.25 Charging-Related Facilities.
   a. Choose whether the system should accept incoming X.25 calls that request reverse charging.
   b. Choose whether outgoing X.25 calls should request reverse charging.

6. Configure the X.25 Restriction Facilities. These facilities are used to place restrictions upon incoming and outgoing X.25 calls.
   a. Choose whether incoming calls should be barred.
   b. Choose whether outgoing X.25 calls should be barred.

7. Configure the X.25 Miscellaneous Facilities.
   a. Choose whether fast select acceptance should be done on incoming calls.
   b. Choose whether fast select should be done on outgoing calls.

After all of the X.25 facilities have been specified, you may configure virtual circuits.

PERMANENT VIRTUAL CIRCUIT INFORMATION

Note: SVCs and PVCs are specified in the X.25 Logical Channel Assignments section of the configuration. However, PVCs require additional configuration, which is done in this section.

1. Follow the onscreen instructions to begin the configuration of a virtual circuit.

Note: Default values are configured for each PVC when an access is newly created. You are given the opportunity to modify the PVC configuration (steps 2 through 7). If you are unsure of what to change, use the default configuration. Note that the packet sizes are limited to 128 bytes for D-channel configurations.

2. Enter the Logical Channel Number (LCN) that is to be used for this PVC. LCN values are obtained from the PPSN carrier.

3. Enter the nonstandard default transmit window size.

4. Enter the nonstandard default receive window size.

5. Select the nonstandard default transmit packet size.

6. Select the nonstandard default receive packet size.

7. Select the nonstandard default transmit throughput class.

8. Select the nonstandard default receive throughput class.

9. After all of the above information has been entered for your PVC, repeat the above steps to add the rest of your PVCs (up to the maximum number of PVCs)

X.25 CONFIGURATION ELEMENTS

X.25 LINE CONFIGURATION ELEMENTS

LINE ID NUMBER

From the displayed list of available lines, this is the Id Number of the previously defined line that is to be used for this X.25 connection. A line that is in use by another type of access will not be available for use by an X.25 access.

X.25 ACCESS NAME

The user defined name that will be used to identify this X.25 access. This name can consist of 1 to 16 non-blank, alpha-numeric characters. The X.25 access name is provided as an aid in helping to track events occurring on an X.25 access.

LOCAL DTE ADDRESS

The X.121 address to be used as the local DTE address. The *X.121 address* is the public data network address assigned by your X.25 provider. The local *DTE* (Data Terminal Equipment) in our application refers to the CyberSWITCH.

DATA RATE

The data rate that applies to the line being used for this X.25 access. The configured data rate can be 56 or 64 Kbps.

BEARER CHANNELS
A list of bearers (a channel map) that will be used on the line associated with this X.25 access. For PRI lines, the range of channels is from 1 to 24.For BRI lines, the range of channels is from 1 to 2. Separate bearer channels by commas, and / or list a range by using a dash (-).

LAPB CONFIGURATION ELEMENTS

Link Access Protocol-Balanced (LAPB), is a data link layer protocol that is used in X.25 connections. LAPB is based on the HDLC protocol.

Note: If you are unsure of any of these values, use the default values where provided.

LAPB SEQUENCE NUMBER RANGE
The LAPB sequence number range to use, regular, or extended. Extended sequence numbering allows for frames to be assigned sequence numbers from 0-127 (modulo 128), as opposed to 0-7 (modulo 8). Using modulo 128, the DTEs can send up to 127 frames without receiving an acknowledgment. Using modulo 8, the DTEs can send up to 7 frames without receiving an acknowledgment. The default value is modulo 8.

TIMER T1
This timer defines the maximum time to wait for responses to pending commands. The range for the T1 timer is 1 to 10 seconds. The default value is 1 second.

TIMER T3
This timer signals that an excessively long idle time is occurring on the link. LAPB requires that Timer T3 be greater than Timer T1. The range for the T3 timer is 2 to 20 seconds. The default value is 10 seconds.

MAXIMUM NUMBER OF FRAME RETRANSMISSIONS
This is the maximum number of frame retransmissions that can be performed (commonly known as "N2"). If this maximum is exceeded, the link is considered out of order. The range for the maximum number of frame retransmissions is 1 to 5 retransmissions. The default value is 3 retransmissions.

MAXIMUM NUMBER OF OUTSTANDING FRAMES
Enter the maximum number of frames that the transmitting station may have outstanding at any given time (commonly known as "K"). The range for this parameter will be 1-7 if the modulo 8 sequence numbers are being used for LAPB, or 1-127 if modulo 128 sequence numbers are being used. The range for the maximum number of outstanding frames is 1 to 7 frames. The default value is seven frames.

X.25 ACCESS CONFIGURATION ELEMENTS

The X.25 Access configuration elements are divided into seven different categories:

- X.25 Logical Channel Assignments
- X.25 Timer Configuration
- X.25 Reliability, Windows, and Acknowledgment Facilities
- X.25 Quality-of-Service Facilities
- X-25 Charging -Related Facilities
- X-25 Restriction Facilities
- X.25 Miscellaneous Facilities

Each category has multiple configuration elements that must be entered.

Note: If you are unsure of any of the configuration values, use the default values where provided.

X.25 LOGICAL CHANNEL ASSIGNMENTS

The maximum number of permanent virtual circuits (PVCs) and switched virtual circuits (SVCs) to be supported. For X.25 over B-channel, a total of 48 virtual circuits are supported; over D-channel 8 virtual circuits are supported. Therefore, the total number of PVCs and SVCs combined cannot exceed the maximum number of VCs. X.25 logical channel numbers are assigned to each PVC, and each two-way SVC. (Currently, one-way incoming and one-way outgoing SVCs are not supported.)

MAXIMUM NUMBER OF PVCS

The maximum number of PVCs supported for this X.25 access.

MAXIMUM NUMBER OF SVCS

The maximum number of SVCs supported for this X.25 access.

X.25 TIMERS

Your PPSN provider should be able to provide you with the optimum values for the X.25 timers. If you are unable to obtain these values, select the default values. The default values are acceptable for the majority of network configurations.

TIMER T20

This timer designates the time limit in which a restart confirmation must be returned by the DCE (the PPSN) after a restart request has been issued by the DTE (the CyberSWITCH). The range for the this timer is 1 to 200 seconds. The default for this timer is 180 seconds.

TIMER T21

This timer designates the time limit in which a call connected response must be returned by the DCE (the PPSN) after a call request has been issued by the DTE (the CyberSWITCH). The range for the this timer is 1 to 200 seconds. The default for this timer is 200 seconds.

TIMER T22

This timer designates the time limit in which a reset confirmation must be returned by the DCE (the PPSN) after a reset request has been issued by the DTE (the CyberSWITCH). The range for the this timer is 1 to 200 seconds. The default for this timer is 180 seconds.

TIMER T23

This timer designates the time limit in which a clear confirmation must be returned by the DCE (the PPSN) after a clear request has been issued by the DTE (the CyberSWITCH). The range for the this timer is 1 to 200 seconds. The default for this timer is 180 seconds.

X.25 Reliability, Windows, and Acknowledgment

X.25 Sequence Number Range

The type of sequence numbers to be used for X.25; regular or extended. Extended sequence numbering allows for packets to be assigned sequence numbers from 0-127 (modulo 128), as opposed to 0-7 (modulo 8). The default value is modulo 8.

Maximum Window Size

This is the largest possible window size to be supported on any virtual circuit. The window size is the number of frames that a DTE can send without receiving an acknowledgment. SVCs that support window size negotiation will never allow the agreed upon window size to exceed this value. Using modulo 128, the DTEs can send up to 127 frames without receiving an acknowledgment. Using modulo 8, the DTEs can send up to 7 frames without receiving an acknowledgment. The default value for both modulo 8 and modulo 128 is 2.

Maximum Packet Size

This value is used to determine the maximum packet size that the system will support for X.25 connections. When packet size negotiation is performed on SVCs, this value will be used as the upper bound. The default maximum packet size is 128 bytes.

X.25 Quality-of-Service Facilities

The X.25 Quality-of-Service Facilities apply only to SVCs. The first three configuration elements are for SVCs that support negotiation.

Maximum Throughput Class

This value is used to determine the maximum throughput class that the system will support for X.25 connections. Throughput describes the maximum amount of data that can be sent through the network, when the network is operating at saturation. Factors influencing throughput are line speeds, window sizes, and the number of active sessions in the network. When throughput class negotiation is performed on SVCs, this value will be used as the upper bound. The default value is 19,200 BPS.

Flow Control Negotiation

This configuration element specifies whether Flow Control Negotiation is to be supported for SVCs (negotiation is not performed on PVCs). If Flow control negotiation is supported for SVCs, the window and packet sizes can be negotiated between DTEs on a per-call basis. As a default, this facility is not supported.

Throughput Class Negotiation

This configuration element specifies whether Throughput Class Negotiation is to be supported for SVCs (negotiation is not performed on PVCs). This facility allows the throughput rates to be negotiated between DTEs on a per-call basis. As a default, this facility is not supported.

Note: The next 6 items configured for the X.25 Quality of Service Facilities are the non-standard default parameters for SVCs that do not support negotiation. These parameters are used on SVCs that do not use the standard X.25 values, but also do not support any facility negotiation.

NONSTANDARD DEFAULT TRANSMIT WINDOW SIZE
The number of frames that a DTE can send without receiving an acknowledgment. Using modulo 128, the DTEs can send up to 127 frames without receiving an acknowledgment. Using modulo 8, the DTEs can send up to 7 frames without receiving an acknowledgment. The default value for both modulo 8 and modulo 128 is 2.

NONSTANDARD DEFAULT RECEIVE WINDOW SIZE
The number of frames that a DTE can receive without receiving an acknowledgment. Using modulo 128, the DTEs can receive up to 127 frames without receiving an acknowledgment. Using modulo 8, the DTEs can send up to 7 frames without receiving an acknowledgment. The default value for both modulo 8 and modulo 128 is 2.

NONSTANDARD DEFAULT TRANSMIT PACKET SIZE
The size of a packet that a DTE can transmit. The choice of a packet size must be weighed against the requirements for larger buffers at all the machines that process the packet. Larger packet sizes reduce the opportunity for other devices to share the channel. On the other hand, a larger packet reduces the ratio of overhead fields to user data. The default transmit packet size is 128 bytes.

NONSTANDARD DEFAULT RECEIVE PACKET SIZE
The size of a packet that a DTE can receive. The choice of a packet size must be weighed against the requirements for larger buffers at all the machines that process the packet. Larger packet sizes reduce the opportunity for other devices to share the channel. On the other hand, a larger packet reduces the ratio of overhead fields to user data. The default transmit packet size is 128 bytes.

NONSTANDARD DEFAULT TRANSMIT THROUGHPUT CLASS
Transmit throughput describes the maximum amount of data that can be sent through the network, when the network is operating at saturation. Factors influencing throughput are line speeds, window sizes, and the number of active sessions in the network. The default value is 19,200 BPS.

NONSTANDARD DEFAULT RECEIVE THROUGHPUT CLASS
Receive throughput describes the maximum amount of data that can be received through the network, when the network is operating at saturation. Factors influencing throughput are line speeds, window sizes, and the number of active sessions in the network. The default value is 19,200 BPS.

X.25 CHARGING-RELATED FACILITIES
These facilities are used to place charging-related restrictions upon incoming and outgoing X.25 calls.

INCOMING CALLS REVERSE CHARGING
This parameters allows you to choose whether the DTE (the CyberSWITCH) should accept incoming X.25 calls that request reverse charging. The default configuration is to not allow incoming X.25 calls to request reverse charging.

OUTGOING CALLS REVERSE CHARGING
This parameters allows you to choose whether the DTE (the CyberSWITCH) should be able to request reverse charging for outgoing calls. The default configuration is to not allow outgoing X.25 calls to request reverse charging.

X.25 RESTRICTION FACILITIES
These facilities are used to place restrictions upon incoming and outgoing X.25 calls.

BARRING INCOMING CALLS
Allows to you bar X.25 calls coming in to the system. The default configuration is to not bar incoming X.25 calls.

BARRING OUTGOING CALLS
Allows you to bar X.25 calls going out of the system. The default configuration is to not bar outgoing X.25 calls.

X.25 MISCELLANEOUS FACILITIES
These facilities are used for fast select acceptance for incoming and outgoing X.25 calls. Fast select is a calling method that allows the device to send a limited amount of information along with a "call request packet" rather than after the packet.

FAST SELECT ACCEPTANCE - INCOMING CALLS
Allows you to chose whether fast select acceptance should be done on incoming calls. The default configuration is to not perform fast select acceptance on incoming calls.

FAST SELECT ACCEPTANCE - OUTGOING CALLS
Allows you to chose whether fast select acceptance should be done on outgoing calls. The default configuration is to not perform fast select acceptance on outgoing calls.

After all of the above X.25 facilities have been specified, the configuration of the X.25 access itself have been completed. You may now configure the virtual circuits associated with the X.25 access.

PVC CONFIGURATION ELEMENTS

Once the above X.25 configuration elements have been configured, the associated virtual circuits should be configured. Note that virtual circuits may be configured with any combination of SVCs and PVCs, adding up to a maximum of 48 virtual circuits.

A PVC is similar to a dedicated line. At subscription time, the subscriber gives the network the address to be associated with that virtual circuit. A logical channel is permanently assigned. From that point on, no call set up is needed. Data to be sent to that destination are simply sent in data packets using the assigned logical channel.

LOGICAL CHANNEL NUMBER (LCN)
X.25 uses LCNs to distinguish the connections between DTEs at either end of a communication. These LCNs make it possible to send a packet into a packet-switched network at one end (with no control over the packet's journey) and then to pick the packet out at the receiving end. LCN values for PVCs are obtained from the PPSN carrier.

NONSTANDARD DEFAULT TRANSMIT WINDOW SIZE
The number of frames that a DTE can send without receiving an acknowledgment. Using modulo 128, the DTEs can send up to 127 frames without receiving an acknowledgment. Using modulo 8, the DTEs can send up to 7 frames without receiving an acknowledgment. The default value for both modulo 8 and modulo 128 is 2.

NONSTANDARD DEFAULT RECEIVE WINDOW SIZE
The number of frames that a DTE can receive without receiving an acknowledgment. Using modulo 128, the DTEs can send up to 127 frames without receiving an acknowledgment. Using modulo 8, the DTEs can send up to 7 frames without receiving an acknowledgment. The default value for both modulo 8 and modulo 128 is 2.

NONSTANDARD DEFAULT TRANSMIT PACKET SIZE
The size of a packet that a DTE can transmit. The choice of a packet size must be weighed against the requirements for larger buffers at all the machines that process the packet. Larger packet sizes reduce the opportunity for other devices to share the channel. On the other hand, a larger packet reduces the ratio of overhead fields to user data. The default transmit packet size is 128 bytes.

NONSTANDARD DEFAULT RECEIVE PACKET SIZE
The size of a packet that a DTE can receive. The choice of a packet size must be weighed against the requirements for larger buffers at all the machines that process the packet. Larger packet sizes reduce the opportunity for other devices to share the channel. On the other hand, a larger packet reduces the ratio of overhead fields to user data. The default transmit packet size is 128 bytes.

NONSTANDARD DEFAULT TRANSMIT THROUGHPUT CLASS
Transmit throughput describes the maximum amount of data that can be sent through the network, when the network is operating at saturation. Factors influencing throughput are line speeds, window sizes, and the number of active sessions in the network. The default value is 19,200 BPS.

NONSTANDARD DEFAULT RECEIVE THROUGHPUT CLASS
Receive throughput describes the maximum amount of data that can be received through the network, when the network is operating at saturation. Factors influencing throughput are line speeds, window sizes, and the number of active sessions in the network. The default value is 19,200 BPS.

X.25 ACCESS BACKGROUND INFORMATION

X.25 was developed to provide an interface that would allow computers or terminals that use different data communications protocols to exchange data across wide area packet-switching networks. Since its inception by CCITT in 1974, it has been expanded to include many options, services, and facilities.

Packet-switching is a transmission method in which data is broken down into packets. The packets are sent across a shared medium from source to destination. The transmission may use any available circuit. The next packet in the transmission may take a different route. Multiple packets from the same transmission can be sent at the same time. Because of the switching, the packets may not all take the same route, and they may not arrive in the order that they were sent. When they arrive at their destination, the packets are reassembled in the proper order, and a check is done to see if all expected packets arrived.

X.25 provides common procedures between a device (DTE) and a packet network (DCE) for establishing a connection to the network, exchanging data with another DTE, and releasing the connection. X.25 contains no algorithms for routing the packets across the wide area network. Consequently, an X.25 Network does not mean that the internal operations of the network use X.25. It simply means that the interface to a packet data network is governed by the X.25 protocol.

Virtual circuits are used to establish a virtual path from one DTE to another. This virtual path appears to have the same characteristics that you might get from a physical telephone circuit. With

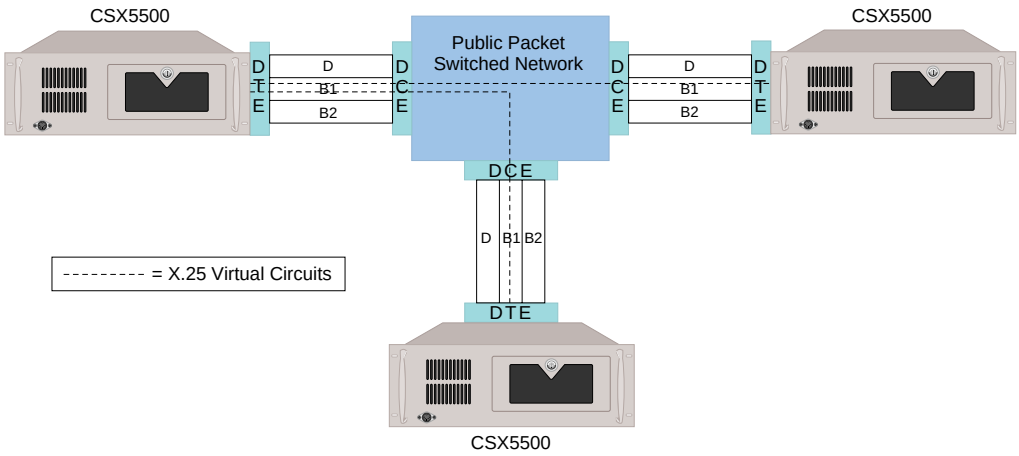
a virtual path, although it appears that a real circuit exits, in reality, the network routes the device's information packets to the designated designation. Any given path may be shared by several devices.

When the virtual circuit is established, a logical channel number is assigned to it at the originating end. A logical channel number is also assigned to the virtual circuit at the destination end, such that at each end there is a one to one correspondence between logical channel number and the virtual circuit. However, the logical channel numbers at each end of a virtual circuit are different.

Two types of virtual circuits can be used: a permanent virtual circuit (PVC) or a switched virtual circuit (SVC). A PVC is similar to a dedicated line. At subscription time, the subscriber gives the network the address to be associated with that virtual circuit. A logical channel is permanently assigned. From that point on, no call set up is needed. Data to be sent to that destination is simply sent in data packets using the assigned logical channel.

A SVC is similar to a dial-up connection. A call origination packet called a Call Request packet, containing the address of the called party, must be given to the network to cause the establishment of the virtual circuit.

As is specified by X.25, multiple logical connections can be multiplexed over a single physical channel. In the case where an ISDN basic rate line is providing the physical channel to a PPSN, multiple X.25 virtual circuits can be present on a single B-channel. The following diagram illustrates that point.



Note: In the illustration, the DTEs are all CyberSWITCH systems. Throughout the X.25 Access section, the term "DTE" can be interchanged with "CyberSWITCH".

Public Packet Switched Networks are typically more cost effective for users who transmit data in the mid-traffic range. Low volume users can incur lower costs using public telephone dial-up than a comparable session in a packet network. At the other end of the spectrum, high volume users are better served with leased lines.

CURRENT X.25 RESTRICTIONS

- X.25 virtual circuits must be two-way logical channels; one-way incoming and one-way outgoing channels are not currently supported.
- Each system can have only one X.25 access. The X.25 access can use only one line.
- A maximum of forty eight virtual circuits can be configured per access. This can be any combination of PVCs or SVCs. Each virtual circuit counts as one of the system's available 48 connections.
- X.25 accesses cannot be changed via Dynamic Management.
- Security must be enabled on the system in order to support X.25 connections.
- Bearer channels which are used by X.25 accesses may not be shared by other access types.
- Support for X.25 Multi-Link Protocol is not provided.
- There can be no aggregation between X.25 virtual circuits and any other type of connections (for example, ISDN, Dedicated, or Frame Relay).
- The maximum X.25 packet size supported is 1024 bytes.
- RFC877 is the only line protocol supported for X.25 VCs. Therefore, only IP data can be sent over an X.25 VC.

FRAME RELAY ACCESSES

CONFIGURING A FRAME RELAY ACCESS

Notes: You may configure up to 32 frame relay accesses per CyberSWITCH, and a total of 192 PVCs. The number of PVCs you can assign per access is arbitrary, as long as the total number of PVCs (from all accesses) is not greater than 192.

Frame relay and X.25 accesses are available only if you have purchased the additional software module for packet switched accesses.

USING CFGEDIT

To add a frame relay access, you need to enter information for the access itself, and also for the associated PVC. A separate section with instructions for completing the configuration of each follows.

Note: If a default value is provided, use that default value if you are unsure of the value.

CONFIGURING GENERAL ACCESS INFORMATION

1. Select *Access* from the *Physical Resources* menu, then follow the onscreen instructions to add a a frame relay access.

2. Enter the *Line Id* the access will be using.

3. Select *Access Information*.

4. Enter a frame relay access name of 1 to 16 non-blank, alpha-numeric characters. The frame relay access name is a user-defined name and is provided as an aid in helping you track events occurring on a Frame Relay Access. (This name will also be reflected in the *Device Table Menu* of the associated remote device.)
5. Select the data rate from the supplied list of data rates.

6. Enter a list of bearers (a channel map). For T1 or PRI lines, the range of channels is from 1 to 24.For BRI lines, the range of channels is from 1 to 2. Separate bearer channels by commas, and / or list a range by using a dash (-).

7. Enter the maximum frame size supported by the network (including the endpoints).

8. Select whether or not HDLC Data is inverted.

9. Enable / disable Link Failure Detection.

10. Indicate whether or not this frame relay access will support the Local Management Interface (LMI).

11. Select the LMI format from the supplied list of formats. The recommended LMI format is CCITT. If this format is unavailable, use ANSI.

12. Indicate whether or not this frame relay access will support CLLM messages.

    Note: CLLM is available only in Japan, and is recommended for systems in Japan. CLLM must be requested from your carrier service.

13. Enter the Link Integrity Verification Timer duration in seconds.

14. Enter the following counts: Full Status Enquiry Polling Count, the Error Threshold Count, and the Monitored Events Count.

Once the above frame relay parameters have been configured, an index number will be assigned to this Access. You will then be returned to the *Access Information/PVC* prompt.

CONFIGURING A PVC

1. From the *Access Information/PVC* prompt, select *PVCs*. The system will display currently-configured PVCs.

2. Select *Add a PVC*.

3. Enter the DLCI for this permanent virtual circuit.

4. Select a PVC line protocol

5. Enter the PVC name. This PVC name should match the name of an associated remote device to be configured in the *Current Device Table*.

6. Enter the Committed Information Rate in Kbits / second.

   Note: Even if you do not wish to pay extra for a CIR from your carrier, we recommend configuring CIR where the following is true:

   physical speed / number of PVCs = CIR

   This configuration will allow quick alleviation of congestion.

7. Enter the Excess Information Rate in Kbits / second.

8. Indicate whether or not Congestion Control should be enabled.

9. Enter the Rate Measurement Interval in msecs.

   Note: You must restart the CyberSWITCH in order to associate the PVC with a device.

After all of the above PVC information is entered, an index number will be assigned to the associated DLCI. This is the index number that should be used when issuing various frame relay access console commands.

You may continue to define PVCs on the currently selected line up to the limit available for this system. The limit is currently a total of 192 PVCs. If you configure more than one Frame Relay access, the total number of PVCs for all accesses can not be greater than 192.

FRAME RELAY GENERAL CONFIGURATION ELEMENTS

Note: If you are unsure of any of any of these values, use the default values where provided.

LINE ID NUMBER

From the displayed list of available lines, the Id Number of the previously defined line that is to be used for this frame relay connection.

FRAME RELAY ACCESS NAME

The user-defined name that will be used to identify this frame relay access. This name can be a string with 1 to 16 characters, using non-blank alpha-numeric characters.

DATA RATE

The data rate that applies to the line being used for this frame relay access.

BEARER CHANNELS

A list of bearers (a channel map) that will be used on the line associated with this frame relay access. This parameter is required for PRI and BRI lines. For PRI lines, the range of bearer channels is from 1 to 24.For BRI lines, the range of bearer channels is 1 to 2. To enter the list of bearer channels, separate the bearer channels by commas, and / or list a range by using a dash (-).

Note: The bandwidth available for this access is equal to the data rate multiplied by the number of bearer channels used by this access. For example, if the configured data rate is 64 Kbps, and 2 bearer channels have been configured, the bandwidth available for this example frame relay access would be 128 Kbps.

MAXIMUM FRAME SIZE

The maximum frame size supported by the network (including the endpoints).

HDLC DATA POLARITY

Indicates whether or not HDLC Data is sent over the line inverted.

LINK FAILURE DETECTION

You may enable or disable link failure detection. If enabled, when Frame Relay detects a link failure, a backup procedure will be followed for the corresponding remote device. Link Failure Detection is only supported across PPP permanent virtual circuits. Some Frame Relay networks

have a per packet charge, therefore, the administrator should be cautious when enabling this feature.

LMI
Indicates whether or not this frame relay access will support the Local Management Interface (LMI). If this frame relay access supports LMI, LMI information can be displayed by entering the *fr lmi* command at the system console prompt. For further LMI information, refer to the *Local Management Interface Overview*.

LMI FORMAT
The LMI format used by this frame relay access. Available formats include ANSI, and CCITT. The recommended LMI format is CCITT. If this format is unavailable, use ANSI.

CLLM MESSAGES
Indicates whether or not this frame relay access will support Consolidated Link Layer Management (CLLM) messages. CLLM is recommended for systems in Japan. CLLM must be requested from your carrier service. The CLLM message is based on the standard Layer 2 XID frame used for the exchange of functional information. If this frame relay access supports CLLM messages, any of these messages that are sent across the network will be included in the system log messages. To access the system log message, enter the *dr* command at the system console prompt.

LINK INTEGRITY VERIFICATION TIMER VALUE
The number of seconds between sending STATUS_ENQUIRY messages. This parameter is a component of the LMI.

FULL STATUS ENQUIRY POLLING COUNT
The number of intervals to elapse before sending a full report STATUS_ENQUIRY message. The length of each interval is equal to the value of the configured Link Integrity Verification Timer. This parameter is a component of the LMI.

ERROR THRESHOLD COUNT
The number of errors in the last "n" events required to declare an alarm. When an alarm is declared, a system message will be logged stating that the alarm is now on. To access system log messages, enter the *dr* command at the system console prompt. The number of events ("*n*") is equal to the value of the configured Full Status Enquiry Polling Count. This parameter is a component of the LMI.

MONITORED EVENTS COUNT
The number of consecutive correct events required to reset an alarm. This parameter is a component of the LMI.

FRAME RELAY PVC CONFIGURATION ELEMENTS

Once the above frame relay parameters have been configured, the associated PVCs should be configured. A frame relay access may have multiple PVCs, within this limit: the aggregate bandwidth of all associated PVCs cannot exceed the bandwidth of the frame relay access.

DLCI VALUE
Each data frame to be transmitted by an endpoint is identified by a Data Link Connection Identifier (DLCI). The DLCI is supplied by the service provider at subscription time. It is a unique identifier for that PVC. The DLCI identifies a pre-established path, or permanent virtual circuit, within the access line to the frame relay network. The frame relay switch at the edge of the frame relay

network, the one to which the access line is directly connected, routes the packet to the intended destination based on the DLCI therein. Hence, each packet is routed independently through the network based on the addressing information provided by this identifier.

PVC LINE PROTOCOL
The PVC line protocol determines which type of data encapsulation will be used on the PVC. The options are PPP Point to Point Protocol or FR_IETF. PPP allows PPP authentication for the associated device. FR_IETF is a multiprotocol encapsulation for Frame Relay, currently specified by RFC 1490. FR_IETF protocols include IP, MAC Layer Bridge, IPX, and AppleTalk. The default PVC line protocol is PPP.

PVC NAME
The PVC name associates the PVC with a device table entry, whether it is defined in an on-node or off-node database. The PVC name must match the device name for both on-node and off-node databases. However, if a virtual circuit has been configured with PPP as the line protocol, and the associated on-node device entry has enabled outbound authentication, then the names are not required to match.

COMMITTED INFORMATION RATE (IN KBITS / SECOND)
A frame relay circuit has two transmission rates associated with it: the Committed Information Rate (CIR) and an Excess Information Rate (EIR). The committed information rate is the bandwidth requested for a PVC at service subscription time. This parameter should be available from the service provider at subscription time. Even if you do not wish to pay extra for a CIR from your carrier, we recommend configuring CIR where the following is true:

physical speed / number of PVCs = CIR

This configuration allows quick alleviation of congestion. For a more in-depth explanation of the Committed Information Rate, refer to the *Data Rate Control Overview*.

EXCESS INFORMATION RATE (IN KBITS / SECOND)
The Excess Information Rate is the bandwidth available above and beyond the committed rate. The frame relay software has the capability to transmit data above the committed information rate up to the excess information rate. This parameter should be available from the service provider at subscription time. For a more in-depth explanation of the Excess Information Rate, refer to *Data Rate Control Overview*.

ENABLE / DISABLE CONGESTION CONTROL
Congestion Control can be enabled or disabled. This parameter should only be disabled for captive networks or those users very familiar with the Frame Relay Service. For a more in-depth Congestion Control explanation, refer to *Congestion Control Overview*.

RATE MEASUREMENT INTERVAL (IN MSECS)
The Rate Measurement Interval in combination with the current transmit or receive rate is used to determine the number of bytes that can be handled in a single rate monitoring period on a given PVC. This parameter should only be changed for those users very familiar with the Frame Relay Service. For a more in-depth explanation, refer to *Data Rate Control Overview*.

FRAME RELAY ACCESS BACKGROUND INFORMATION

Frame Relay is a frame mode service in which data is switched on a per frame basis, as opposed to a circuit mode service that delivers packets on a call-by-call basis. This feature will allow the system to efficiently handle high-speed, bursty data over wide area networks. It offers lower costs and higher performance than a X.25 packet switched network for those applications that transmit data at a high speed in bursts.

In private line network implementations, network bandwidth is dedicated to a particular destination, whether via private lines or circuit switched connections. In any event, these resources are only available to traffic bound for that location and are reserved for that traffic whether that traffic is present or not. Conversely, in a frame relay network, bandwidths within the network and in the access lines are only allocated between any two end devices if there is traffic moving between those devices. At other times, this bandwidth is made available to other network devices. Therefore, the performance in a frame relay network is then only limited by the bandwidth available at the access point to the frame relay network and not necessarily by any preallocated end-to-end bandwidth as would be the case of a private line network. In a manner of speaking, this provides bandwidth on demand since network bandwidth is allocated to this data path (virtual circuit) only when traffic is present.

Bandwidth is provided by the network's Permanent Virtual Circuit (PVC) service: each data frame to be transmitted by an endpoint contains and is identified by a Data Link Connection Identifier (DLCI). The DLCI identifies a pre-established path, or permanent virtual circuit, within the access line to the frame relay network. The frame relay switch at the edge of the frame relay network, the one to which the access line is directly connected, routes the packet to the intended destination based upon the DLCI therein. Hence, each packet is routed independently through the network based on the addressing information provided by this identifier.

The two line protocols used for data encapsulation on a permanent virtual circuit are Point to Point Protocol or FR_IETF. PPP specifies the operation of the PPP protocol over Frame Relay links. Although the CyberSWITCH supports this method of encapsulation, Inband Protocol Demultiplexing is not performed when a PVC is initiated because the system statically configures the line protocol used for a PVC. FR_IETF is a multiprotocol encapsulation for Frame Relay, currently specified by RFC 1490. FR_IETF protocols include IP, MAC Layer Bridge, IPX, and AppleTalk.

Although Frame Relay is transparent to each of the protocols specified by FR_IETF, there are a few special considerations to note. ARP, RARP, and IARP are protocols provided by FR_IETF for IP over Frame Relay. These protocols are used to determine the IP and DLCI information used on the virtual circuits. However, since this information is configured in the CyberSWITCH, these protocols are not supported. The CyberSWITCH's implementation of FR_IETF supports the Bridge Point to Point model. The Virtual port model or Extended Spanning Tree is not supported.

The PVC name associates the permanent virtual circuit with a device table entry, whether it is defined in an on-node or off-node database. If an on-node device database is used, the PVC name must match the device name if outbound authentication has been disabled for a device associated with a PPP virtual circuit, or if FR_IETF has been configured as the line protocol. However, if outbound authentication has been enabled for a PPP device, the PVC name isn't required to match. If an off-node device database is used, the PVC name must match the device name for both line protocols. FR_IETF requires that all PVC names match a configured device database entry, since no identification mechanism is provided by this line protocol. When upgrading from a previous release of the UAA software, the CyberSWITCH will process the previous PVC name, which was

configured in the device table. It will find the PVC and the line protocol that corresponds to the PVC name and change its PVC name to match the corresponding device name.

Notes: Connection Services Manager (CSM) is currently the only off-node device database supported by the CyberSWITCH for Frame Relay.

The management of Frame Relay permanent virtual circuits requires the use of some form of security. Therefore, systems with frame relay remote devices cannot select No Security for the security level.

Frame Relay uses ISDN to provide backup redundancy for failed Frame Relay links. In the event that a Frame Relay link fails, an ISDN call is brought up and all traffic that was to be forwarded on the Frame Relay link is forwarded over the ISDN call. Once the Frame Relay link comes back up the ISDN call will be taken down and transmission of data will resume over the Frame Relay link.

When using FR_IETF data encapsulation, LMI is used to determine the status of failed Frame Relay virtual circuits. When using PPP data encapsulation, Link Failure Detection can be enabled for the Frame Relay access. Link Failure Detection is only supported across PPP permanent virtual circuits. Some Frame Relay networks have a per packet charge, therefore, the administrator should be cautious when enabling this feature.

The three main operational components of a frame relay access are the Local Management Interface (LMI), Data Rate Control, and Congestion Control. The following three sections provide an overview of the role that each of these components plays in the function of frame relay access.

THE LOCAL MANAGEMENT INTERFACE OVERVIEW

Besides the steady state data transfer portion of the frame relay module, the standards have provided for a frame relay management function, known as the Local Management Interface (LMI). The purpose of this interface is to provide a controlled means of verifying both link integrity and the network status of all PVCs configured on the frame relay access defined by a given physical link.

The elements of this management interface are the STATUS and STATUS_ENQUIRY messages. The STATUS_ENQUIRY messages are sent out by the user equipment at regular intervals. The interval at which these status messages are sent, the polling interval, is a configurable value. The network will respond to these STATUS_ENQUIRY messages with its own STATUS message containing a link integrity verification information element. The user equipment will request via the STATUS_ENQUIRY either a Link Integrity Verification STATUS message from the network or a full report STATUS message. The link integrity verification STATUS message simply functions as a signal to verify that the link is still operable. This full report signals the user equipment when a PVC is no longer usable, and also when a previously non-active PVC has become available.

DATA RATE CONTROL OVERVIEW

To handle congestion within the network and at the endpoints, the frame relay protocol provides certain congestion control features.

A frame relay PVC has two transmission rates associated with it: the Committed Information Rate (CIR) and an Excess Information Rate (EIR). The committed information rate is the bandwidth requested for a PVC at service subscription time. It is essentially the guaranteed transmission rate

-- the rate at which data frames may be sent into the network without incurring congestion. This is generally accepted as the end-to-end available bandwidth at which frame relay service devices may enjoy sustained frame transmission. By definition this must be less than the throughput that the actual physical access link can support. However, for short periods of time, service devices may exceed this rate by defined values. This excess is known as the excess information rate and is defined as the bandwidth available above and beyond the committed rate. The reason this is possible is because statistically, not each PVC within the access will make use of its complete bandwidth allocation. Busy PVCs may essentially borrow bandwidth from underutilized PVCs. The Frame Relay software has the capability to transmit data above the committed information rate up to the excess information rate. Note that the sum of the committed and the excess information rates must not exceed the rate defined by the physical link. These rates are user-configurable options.

CONGESTION CONTROL OVERVIEW

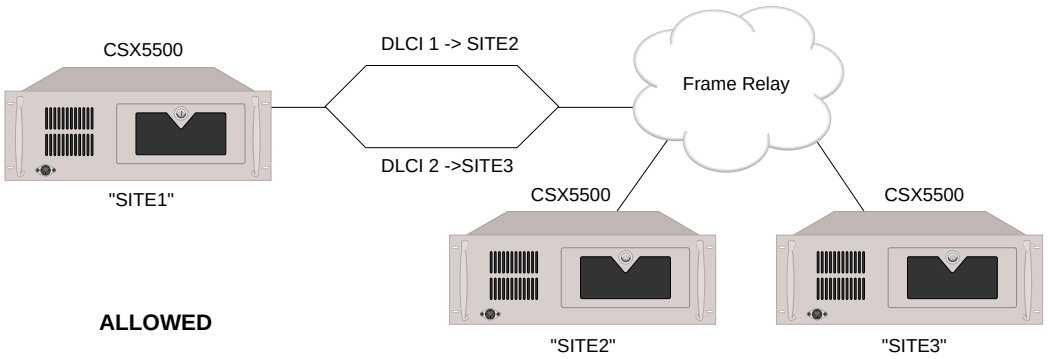
Congestion occurs when traffic arriving at a resource, whether network or user equipment, exceeds that node's capacity. Congestion notification in the device plane is used to inform the equipment (at the ingress point to the network) of the congestion, and allows the user equipment to initiate congestion avoidance procedures. The intent is to reduce the negative effects on both network and user equipment: the user equipment should take corrective action to reduce the congestion, or to notify the source that throughput has been exceeded. Congestion control is very important in providing reliable frame relay services. Congestion can be detected in two ways, implicitly and explicitly. Implicit indications are provided by lost frames whereas explicit congestion indications are provided for within the frame relay protocol.

CURRENT RESTRICTIONS

Currently, only PVC (Permanent Virtual Circuit) frame relay connections are implemented. Through configuration, PVC connections establish a permanent association between two DTEs.

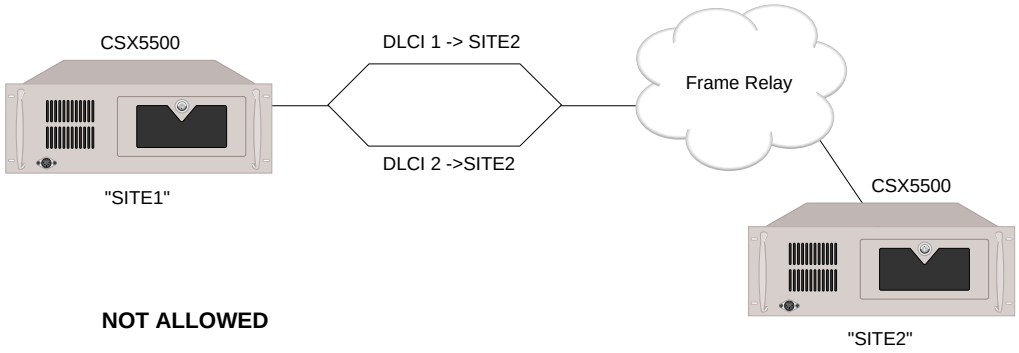
The only types of facilities to be supported for frame relay access are serial interfaces (such as V.35 and RS-232) and channeled interfaces such as T1 / PRI and BRI. However, currently only 1 port per channeled interface is supported until SVC standards are available.

Frame relay supports only a single Permanent Virtual Circuit connecting any two given CyberSWITCH systems. To illustrate this point, the following diagram shows a frame relay network configuration that would be allowed:



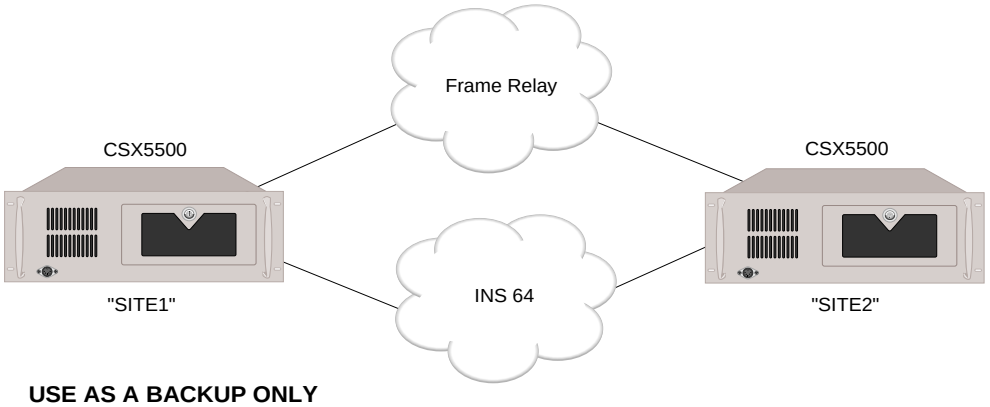
ALLOWED

However, under the above stated conditions, the network configuration shown below would not be allowed:



NOT ALLOWED

Switched connections can only be used as a backup to frame relay. As such, a switched connection would be made to a given node connected by a frame relay access only after that frame relay access had failed. Switched and packet mode services will not be allowed to connect any given two nodes simultaneously. The following diagram is provided as an example. The INS 64 connection between sites SITE1 and SITE2 would only be made if the frame relay connection was somehow lost.



USE AS A BACKUP ONLY

CONFIGURING ADVANCED BRIDGING

OVERVIEW

When bridging is enabled, optional advanced features are available. Optional bridging features include:

- bridge dial out
- Spanning Tree Protocol
- mode of operation
- bridging filters
- known connect lists

This chapter includes a section for each advanced bridging feature.

BRIDGE DIAL OUT

With bridging enabled, bridge dial out is supported. Bridge dial out allows the CyberSWITCH to initiate connections to bridge devices at remote sites. The system accepts bridge data received on the Ethernet LAN or ISDN network, and initiates a data connection to a bridge device specified in the device data.

Standard bridge processing attempts to forward non-local MAC frames to configured devices if a connection is up. Now, with the bridge dial out feature, the system will initiate the call, if necessary, through the use of bridge filters or a Known Connect list. Refer to the *Bridge Filters* section and the *Known Connect List* section for further information.

The "bridge" determines if a connection already exists, or whether a connection should be initiated. The MAC frame is simply forwarded if a connection already exists. If a connection does not, the CyberSWITCH will map the Bridge Address or Dial Out Device Name to a phone number, and initiate a connection. The normal connection processing, protocol negotiation, and data forwarding mechanisms are followed once the connection is requested.

The CyberSWITCH handles bridge dial out as follows:

- If a filter exists, the system checks the filter first. The system will take action on the packet based on the filter.
- If no filter exists, or if no action is taken on the packet based on the filter, the system checks the status of the Known Connect list next. If the packet's destination address corresponds to a device on the Known Connect list, and the packet meets other dial out requirements, the packet is forwarded.

Each of these procedures requires a properly configured Device List. This Device List may be configured locally, or it may be configured on an off-node authentication server.

CONFIGURING THE DEVICE LIST FOR BRIDGE DIAL OUT

Note: The *Configuring Device Level Databases* chapter contains the information needed to completely configure an on-node device entry. The following section provides instructions for entering on-node device information specific to the bridge dial out feature.

USING CFGEDIT

1. Select *Security* from the main menu.
2. Select *Device Level Databases* from the security menu.
3. Enable the On-node Device Database if it is currently disabled.
4. Select *On-node Device Entries* from the authentication database menu.
5. Select *Add*. Provide the device name, as prompted, and continue with device configuration, as described in *Configuring Device Level Databases*:

```
Device Table Menu: (Device = "DAN")

   1)  ISDN
   2)  Frame Relay
   3)  X.25
   4)  Digital Modem
   5)  Authentication
   6)  IP
   7)  IPX
   8)  AppleTalk
   9)  Bridge
   10) Compression

Select function from above or <RET> for previous menu: 1
```

6. Under *ISDN*, select *Dial Out Phone Number*:

```
Device ISDN Menu: (Device = "DAN")

   1) ISDN Line Protocol.       "PPP (Point to Point Protocol)"
   2) Base Data Rate.           "64000 bps"
   3) Initial Data Rate.        "64000 bps"
   4) Maximum Data Rate.        "128000 bps"
   5) Dial Out Phone Number(s). ""
   6) Subaddress.               ""
   7) Profile Name.             "Default_Profile"
   8) H0 Call Support           DISABLED

Id of option to change or press <RET> for previous menu: 5
```

7. Provide device's dial out phone number, as prompted.
8. Return to the *Device Table Menu*, and select *Bridge*:

```
Device Bridging: (Device = "DAN")

   1) IP (sub)network number       None
   2) Bridging                     ENABLED
   3) Make Calls for bridge data   None
   4) IPX Network Number           None
   5) IPX Spoofing Options

Id of option to change or press <RET> for previous menu? 3
```

9. Enable *Bridging*.

10. Enable *Make Calls for bridge data*. You must have already configured the device's phone number (Step 6) before the system allows you to enable this feature.

Return to the Current Device Table. The system notifies you of proper configuration for your new device, or informs you of what you are missing.

SPANNING TREE PROTOCOL

CONFIGURING SPANNING TREE PROTOCOL

USING CFGEDIT

Note: Although the Spanning Tree Protocol is supported for Ethernet-2 adapters only; the Spanning Tree bridge address table aging time can be set for any Ethernet adapter.

1. Select *Spanning Tree* from the Bridging menu.

2. If your CyberSWITCH has an Ethernet-1 adapter, enter the bridge age time. If your CyberSWITCH has an Ethernet-2 adapter, continue with step 3.

3. To configure the Spanning Tree elements, make sure Spanning Tree Protocol is enabled. Follow the on-screen instructions for enabling it if it is disabled.

4. Enter the LAN port priorities.

5. Enter the LAN port path costs.

6. Enter the bridge maximum age-time.

7. Enter the bridge hello time interval.

8. Enter the bridge forward delay time if this system is the root bridge.

9. Enter the bridge age time.

SPANNING TREE PROTOCOL CONFIGURATION ELEMENTS

Only the Ethernet-2 adapter supports the Spanning Tree Protocol in its entirety. Outlined below are the Spanning Tree configuration elements that the User can define. These elements are available when the system is running the local bridging option.

SPANNING TREE PROTOCOL OPTION STATUS

You can enable or disable the Spanning Tree protocol for CyberSWITCHes with Ethernet-2 adapters.

BRIDGE PRIORITY

The configured priority for this system. The priority can range from 0 to 65535. The default is 32768.

LAN PORT <1 OR 2> PRIORITY

The configured priority for the indicated port.The priority can range from 0 to 255. The default is 128.

LAN PORT <1 OR 2> PATH COST

The configured path cost for this port. The cost can range from 1 to 65535. The default is 100.

BRIDGE MAX AGE

The configured maximum age-time for this system. This is used when the system is the root bridge. The unit of age is in seconds, and ranges from 6 to 40. The default is 20 seconds.

BRIDGE HELLO TIME

The configured hello time interval for this system. This is used when the system is the root bridge. The unit is in seconds, and ranges from 1 to 10. The default is 2 seconds.

BRIDGE FORWARD DELAY

The configured forward delay time for this system. This is used when the system is the root bridge. The unit is in seconds and range from 4 to 30. The default is 15 seconds.

This parameter is available on systems with Ethernet-1 or Ethernet-2 adapters. If you are using bridge dial out, you may wish to increase this value to prevent the connection from aging out before the call is made.

SPANNING TREE PROTOCOL BACKGROUND INFORMATION

Spanning Tree Protocol is used to find paths among networks. The algorithm can generate all possible paths and choose one. If that path becomes unavailable because a device goes down, an alternate path is found. This algorithm is used by bridges to find the best path between devices, and to make sure that no path loops occur. For a more detailed explanation of the Spanning Tree protocol, refer to the 802.1d specification available from IEEE.

BRIDGE MODE OF OPERATION

CONFIGURING THE BRIDGE MODE OF OPERATION

USING CFGEDIT

1. Select *Mode of Operation* from the Bridging menu.

2. Select the bridge mode of operation. The unrestricted bridge mode is the default.

BRIDGE MODE OF OPERATION CONFIGURATION ELEMENTS

BRIDGE MODE
The forwarding method that the bridge will use to distribute LAN packets to the remote sites and to the LAN ports of the CyberSWITCH. The default value is unrestricted bridging.

BRIDGE MODE OF OPERATION BACKGROUND INFORMATION

Selecting the bridge mode of operation allows you to determine the forwarding method that the bridge will use to distribute LAN packets to the remote sites and to the LAN ports of the system. The two possible modes of operation are the Unrestricted Bridge Mode and the Restricted Bridge Mode.

Note: If the mode of operation is changed, any previously defined filters will be deleted. Any previously defined protocol definitions will remain unchanged.

The following two sections provide further details for each bridge mode of operation.

UNRESTRICTED BRIDGE MODE

In general, Unrestricted Mode forwards all packets, unless specified otherwise through a bridge filter. If the Unrestricted Bridge Mode is selected, the following packet forward possibilities exist:

- If the packet matches a discard filter, it is discarded.
- If the packet matches a connect filter, it is connected and forwarded to the members of the distribution list.
- If the packet matches no filter, the packet is forwarded. The specific forwarding action depends upon whether or not the destination is known. (See following descriptions.)

  No Filter Match - Destination Known
  If the destination is known and the corresponding device is on the Known Connect List, the connection is made and the packet is then forwarded to the specific destination.

  If the device is not on the Known Connect list, the packet is sent to all current connections.

  No Filter Match - Destination Unknown
  The packet is sent to all current connections.

RESTRICTED BRIDGE MODE

If the Restricted Bridge Mode is selected, packets will be discarded unless overridden by a user-defined bridge filter. The bridge filters, therefore, allow you to transfer only the packets that you specify.

If the Restricted Bridge Mode is selected, the following packet forwarding possibilities exist:

- If the packet matches a discard filter (packet filter only), it is discarded.
- If the packet matches a forward filter, it is forwarded to the distribution list.
- If the packet matches a connect filter, it is connected to the members of the distribution list. However, with Restricted Mode, the packet needs to match a forwarding filter in order to be forwarded.
- If the packet matches no filter, the specific action for the packet depends upon whether or not the destination is known. (See following descriptions.)

  No Filter Match - Destination Known
  If the destination is known and the corresponding device is on the Known Connect list, the connection is made. If the device is not on the Known Connect list, the packet is discarded.

  No Filter Match - Destination Unknown
  The packet is discarded.

BRIDGE FILTERS

CONFIGURING BRIDGE FILTERS

Note: Bridge dial out calls can be initiated through the use of a Known Connect list or through the use of bridge filters. For a description of bridge dial out through bridge filters, refer to the section titled *Dial Out Using Bridge Filters*.

USING CFGEDIT

1. Select *Bridge Filters* from the Bridging menu.

2. Configure any needed protocol definitions. These definitions will be used if you configure any protocol filters. To configure a protocol definition:
   a. Select to add a protocol definition.
   b. Enter a user-defined name for the protocol definition.
   c. Enter the Ethernet type in hex.
   d. Enter the LSAP in hex.

3. Configure source MAC filters.
   a. Select to add a MAC filter.
   b. Enter the source MAC address.
   c. Select a distribution list.

4. Configure destination MAC filters.
   a. Select to add a destination MAC filter.
   b. Enter the destination MAC address.
   c. Select a distribution list.

5. Configure protocol filters.
   a. Select to add a protocol filter.
   b. Select a protocol definition Id.
   c. Select a distribution list.

6. Configure packet data filters.
   a. Select to add a packet data filter.
   b. Enter the off set value.
   c. Enter the mask in hex.
   d. Enter the data value in hex.
   e. Select a distribution list.

USING MANAGE MODE COMMANDS

Manage Mode can be used to complete all of the bridge filter configuration. This section provides you with the commands available for each bridge filter type.

Protocol Definition Commands

protdef
Displays the current protocol definition configuration data.

protdef add
Allows a protocol definition to be added to the current configuration. Refer to the Using CFGEDIT section for required configuration elements (page 269). Configure any needed protocol definitions (page 273).

protdef change
Allows the current protocol definition configuration to be changed.

protdef delete
Allows a protocol definition to be deleted from the current configuration.

Source MAC Filter Commands

srcfilt
Displays the current source address filter configuration data.

srcfilt add
Allows a source address filter to be added to the current configuration. Refer to the Using CFGEDIT section for required configuration elements (page 269).

srcfilt change
Allows the current source address filter configuration to be changed.

srcfilt delete
Allows a source address filter to be deleted from the current configuration.

Destination MAC Filter Commands

destfilt
Displays the current destination address filter configuration data.

destfilt add
Allows a destination address filter to be added to the current configuration. Refer to the Using CFGEDIT section for required configuration elements (page 269).

destfilt change
Allows the current destination address filter configuration data to be changed.

destfilt delete
Allows a destination address filter to be deleted from the current configuration.

Protocol Filter Commands

protfilt
Displays the current protocol filter configuration data.

protfilt add
Allows a protocol filter to be added to the current configuration. Refer to the CFGEDIT section for required configuration elements (page 270).

protfilt change
Allows the current protocol filter configuration to be changed.

protfilt delete
Allows a protocol filter to be deleted from the current configuration.

Packet Data Filter Commands

pktfilt
Displays the current packet filter configuration data.

pktfilt add
Allows a packet filter to be added to the current configuration. Refer to the CFGEDIT section for required configuration elements (page 270).

pktfilt change
Allows the current packet filter configuration to be changed.

pktfilt delete
Allows a packet filter to be deleted from the current configuration.

BRIDGE FILTER CONFIGURATION ELEMENTS

PROTOCOL DEFINITION CONFIGURATION ELEMENTS

PROTOCOL NAME
A user-defined name for the protocol to be filtered. It can be from 1 to 17 alphanumeric characters in length.

ETHERNET TYPE IN HEX
A four digit hexadecimal number (from 0600 to FFFF) that checks the protocol Id of a MAC frame.

LSAP IN HEX
A four digit hexadecimal number (from 0000 to FFFF) that checks the protocol Id of a MAC frame.

BRIDGE FILTER CONFIGURATION ELEMENTS

FILTER ACTION
For each filter category, there are three filtering actions that the system can perform on a packet: discard, forward, or connect the packet.

MAC-ADDRESS
An assigned Media Access Control address as defined by IEEE 802.3 specifications. MAC-addresses are specified as 12 character hexadecimal numbers.

MULTICAST ADDRESS
A Media Access Control address with the group bit set to 1.

DISTRIBUTION LIST
A distribution list is defined as the WAN and/or LAN ports to which the filter action will be applied. The distribution list is selected from a displayed list of possible choices (LAN, WAN, Device Table, or all destinations).

MASK
Hexadecimal number up to 80 characters in length that specifies which bits in the data packets are significant. There must be an even number of hexadecimal digits in the number. A scale will be displayed to help you enter the Mask accurately.

DATA VALUE
Hexadecimal number up to 80 characters in length that specifies the value used to determine if the packet matches the filter. The value field must be a subset of the mask field. That is, the value field logically "anded" with the mask field must be equal to the value field. The value and mask fields must have equal lengths. There must be an even number of hexadecimal digits in the number.

PACKET OFFSET
A decimal number between 1 and 100 that indicates the starting offset in a data packet where a packet filter will begin its data comparison.

PROTOCOL-ID
The symbolic name for the Ethernet protocol to be filtered. The protocol-Id is selected from a displayed list of previously defined protocols. (Refer to the section titled *Protocol Definitions*.)

BRIDGE FILTERS BACKGROUND INFORMATION

User-defined bridge filters allow you to filter unwanted traffic out of the network. The following table lists the four different types of bridge filters and the maximum number of filters that can be configured for each type:

Filter Type	*Maximum Number of Each*
source MAC address filter	50
destination MAC address filter	50
protocol filter	40
packet data filter	60
hardware filter	63 (in manual mode)

Note: If the mode of operation is changed, any previously defined filters will be deleted. Any previously defined protocol definitions will remain unchanged.

MAC address filters reference either the source or destination MAC address fields in a packet. Protocol filters use the protocol Id field in a packet. Packet data filters reference data outside the address and protocol fields in a packet. Each filter has a distribution list that identifies the potential destinations for a filtered packet.

For each filter category, there are three filtering actions that the system can perform on a packet: discard, forward, or connect.

PROTOCOL DEFINITIONS

If you configure any protocol filters, you must first configure any needed protocol definitions. After you define a protocol filter, it will automatically be assigned a protocol Id. The protocol Id is a required field when configuring a protocol filter.

You can define up to 10 protocol definitions. These definitions represent the protocol Id tokens for the protocol filter commands to use. Users specify the protocol name, and also the protocol Id value for the Ethernet type field and / or the 802.3 LSAP field.

Inspecting the 13th and 14th bytes of the MAC frame determines the packet format. These bytes are the length field in an 802.3 format frame, and are the Ethernet type field in an Ethernet format frame. If the value of the byte is less than hexadecimal 600, the packet is 802.3 format and the LSAP field is used for the protocol Id. If the value is greater than or equal to hexadecimal 600, the packet is Ethernet format and the Ethernet type field is used for the protocol Id.

Two of the more common protocols used today are:

- The *IP Protocol Id*, which identifies DOD Internet Protocol packets with Ethernet type equal to hexadecimal 800, or 802.3 LSAP equal to hexadecimal 6060.
- The *IPX Protocol Id*, which identifies Novell (old) NetWare IPX packets with Ethernet type equal to hexadecimal 8137, or 802.3 LSAP equal to hexadecimal E0E0.

BRIDGE FILTER DEFINITIONS

This section provides the syntax for the bridge filters available for the unrestricted bridge mode and the restricted bridge mode.

Unrestricted Mode Bridge Filters

Unrestricted Mode Type of Filter available	*Forwarding Action*
SOURCE	DISCARD
SOURCE	CONNECT
DESTINATION	DISCARD
DESTINATION	CONNECT
PROTOCOL	DISCARD
PROTOCOL	CONNECT
PACKET	DISCARD
PACKET	CONNECT

1. SOURCE unicast-address DISCARD < distribution list >
   This filter allows you to restrict the access privileges of a given device. When the specified unicast address appears in the source address field of a MAC frame, the frame will NOT be forwarded as specified in the distribution list. If no distribution list is specified, the frame will not be forwarded at all. In this manner, you can specify remote sites and LANs to which the device cannot talk.

2. SOURCE unicast-address CONNECT < distribution list >
   This filter allows you to stipulate access privileges of a given device. When the specified unicast address appears in the source address field of a MAC frame, the frame will be connected and forwarded as specified in the distribution list. In this manner, you can specify remote sites and LANs for connection.

3. DESTINATION MAC-address DISCARD < distribution list >
   This filter allows you to discard MAC frames addressed to the specified MAC address. When the specified MAC address appears in the destination address field of the MAC frame, the frame will NOT be forwarded as specified in the distribution list. If no distribution list is specified, the frame will not be forwarded.

4. DESTINATION MAC-address CONNECT< distribution list >
   This filter allows you to connect MAC frames addressed to the specified MAC address. When the specified MAC address appears in the destination address field of the MAC frame, the frame will be forwarded as specified in the distribution list.

5. PROTOCOL protocol-Id DISCARD < distribution list >
   This filter allows you to discard packets based on the Ethernet type field or the corresponding 802.3 LSAP field. You specify the protocol Id that is to be discarded. The filtering mechanism will determine if the packet is Ethernet format or 802.3 format. The Ethernet type or LSAP field will be checked based on packet format. See the section titled "Protocol Definitions" for more information.

6. PROTOCOL protocol-Id CONNECT< distribution list >
   This filter allows you to connect packets based on the Ethernet type field or the corresponding 802.3 LSAP field. You specify the protocol Id that is to be connected. The filtering mechanism will determine if the packet is Ethernet format or 802.3 format. The Ethernet type or LSAP field will be checked based on packet format. See the section titled “Protocol Definitions” for more information.

7. PACKET OFFSET dd MASK xxxxxxxxxxxx VALUE xxxxxxxxxxxx DISCARD <distribution-list>
   This filter allows you to discard packets based on packet data outside the source and destination MAC addresses or protocol Id. For example, you may wish to filter packets based on IP address information. You would then specify the offset (dd) into the MAC frame where the filter comparison is to begin. The mask data indicates which bits within the frame data are significant and will be compared to the value. The frame data is logically “anded” with the mask, and then compared to the specified value. The value field must be a subset of the mask field. That is, the value field logically “anded” with the mask field must equal the value field. The value and mask fields must have equal lengths.

8. PACKET OFFSET dd MASK xxxxxxxxxxxx VALUE xxxxxxxxxxxx CONNECT <distribution-list>
   This filter allows you to connect packets based on packet data outside the source and destination MAC addresses or protocol Id. For example, you may wish to filter packets based on IP address information. You would then specify the offset (dd) into the MAC frame where the filter comparison is to begin. The mask data indicates which bits within the frame data are significant and will be compared to the value. The frame data is logically “anded” with the mask, and then compared to the specified value. The value field must be a subset of the mask field. That is, the value field logically “anded” with the mask field must equal the value field. The value and mask fields must have equal lengths.

The following charts summarize the filter actions available for Unrestricted Bridging:

Filter Action	*Distribution List*	*Result*
DISCARD	LAN	A packet matching this filter will not be forwarded on any LAN port. The packet will be sent to remote sites connected over the WAN according to the normal learning bridge methods.
DISCARD	WAN	A packet matching this filter will not be forwarded to any remote sites connected on the WAN. The packet will be sent to the LAN ports according to the normal learning bridge methods.
DISCARD	ALL	A packet matching this filter will not be forwarded on any LAN port and will not be forwarded to remote sites connected over the WAN.
DISCARD	Device List*	A packet matching this filter will not be forwarded to any sites on the specified Device List.
CONNECT	Device List*	A packet matching this filter will be connected and forwarded to the sites on the specified Device List.

For Unrestricted Bridging, the following additional filter actions are available only on a system with an Ethernet-2 adapter executing the local bridge option.

Filter Action	*Distribution List*	*Result*
DISCARD	LAN PORT 1	A packet matching this filter will not be forwarded on LAN port 1. The packet will be sent to remote sites connected over the WAN and to LAN port 2 according to the normal learning bridge methods.
DISCARD	LAN PORT 2	A packet matching this filter will not be forwarded on LAN port 2. The packet will be sent to remote sites connected over the WAN and to LAN port 1 according to the normal learning bridge methods.
DISCARD	LAN PORT 1 and WAN	A packet matching this filter will only be forwarded on LAN port 2 according to the normal learning bridge methods. The packet will not be sent to remote sites connected over the WAN or to LAN port 1.
DISCARD	LAN PORT 2 and WAN	A packet matching this filter will only be forwarded on LAN port 1 according to the normal learning bridge methods. The packet will not be sent to remote sites connected over the WAN or to LAN port 2.
DISCARD	Device List*	A packet matching this filter will not be forwarded to any sites on this Device List.
CONNECT	Device List*	A packet matching this filter will be connected and forwarded to the sites on the specified Device List.

* *Device List* may be the on-node device database, or it may be located on an off-node authentication server.

Restricted Mode Bridge Filters

Restricted Mode Type of Filter available	*Forwarding Action*
SOURCE	FORWARD
SOURCE	CONNECT
DESTINATION	FORWARD
DESTINATION	CONNECT
PROTOCOL	FORWARD
PROTOCOL	CONNECT
PACKET	FORWARD
PACKET	DISCARD
PACKET	CONNECT

1. SOURCE unicast-address FORWARD <distribution list>
   This filter allows you to stipulate access privileges of a given device. When the specified unicast address appears in the source address field of a MAC frame, the frame will be forwarded as specified in the distribution list. In this manner, you can specify remote sites and LANs for connection

2. SOURCE unicast-address CONNECT < distribution list >
   This filter allows you to stipulate access privileges of a given device. When the specified unicast address appears in the source address field of a MAC frame, the frame will be connected and forwarded as specified in the distribution list. In this manner, you can specify remote sites and LANs for connection.

3. DESTINATION MAC-address FORWARD <distribution list>
   This filter allows you to forward MAC frames addressed to the specified MAC address. When the specified MAC address appears in the destination address field of the MAC frame, the frame will be forwarded as specified in the distribution list.

4. DESTINATION MAC-address CONNECT< distribution list >
   This filter allows you to connect MAC frames addressed to the specified MAC address. When the specified MAC address appears in the destination address field of the MAC frame, the frame will be connected and forwarded as specified in the distribution list.

5. PROTOCOL protocol-Id FORWARD < distribution list >
   This filter allows you to restrict packets based on the Ethernet protocol Id field or the corresponding 802.3 LSAP field. You can specify the protocol Id that is to be forwarded. The filtering mechanism will determine if the packet is Ethernet format or 802.3 format. The Ethernet type or LSAP field will be checked based on packet format.

6. PROTOCOL protocol-Id CONNECT < distribution list >
   This filter allows you to restrict packets based on the Ethernet protocol Id field or the corresponding 802.3 LSAP field. You can specify the protocol Id that is to be connected and then forwarded. The filtering mechanism will determine if the packet is Ethernet format or 802.3 format. The Ethernet type or LSAP field will be checked based on packet format. See the section titled *Protocol Definitions* for more information.

7. PACKET OFFSET dd MASK xxxxxxxxxxxx VALUE xxxxxxxxxxxx FORWARD <distribution-list>
   This filter allows you to restrict packets based on packet data outside the source and destination MAC addresses or protocol Id. For example, you may wish to filter packets based on IP address information. You would then specify the offset (dd) into the MAC frame where the filter comparison is to begin. The mask data indicates which bits within the frame data are significant and will be compared to the value. The frame data is logically "anded" with the mask, and then compared to the specified value. The value field must be a subset of the mask field. That is, the value field logically "anded" with the mask field must equal the value field. The value and mask fields must have equal lengths.

8. PACKET OFFSET dd MASK xxxxxxxxxxxx VALUE xxxxxxxxxxxx CONNECT <distribution-list>
   This filter allows you to restrict packets based on packet data outside the source and destination MAC addresses or protocol Id. For example, you may wish to filter packets based on IP address information. You would then specify the offset (dd) into the MAC frame where the filter comparison is to begin. The mask data indicates which bits within the frame data are significant and will be compared to the value. The frame data is logically "anded" with the mask, and then compared to the specified value. The value field must be a subset of the mask field. That is, the value field logically "anded" with the mask field must equal the value field. The value and mask fields must have equal lengths.

9. PACKET OFFSET dd MASK xxxxxxxxxxxx VALUE xxxxxxxxxxxx DISCARD <distribution-list>
   This filter allows you to specify the DISCARD filter action on a packet data filter. This gives you the flexibility of allowing a global class of data to be forwarded, and restrict specific subsets of that data. For example you may forward all IPX data packets but restrict workstation watchdog packets.

The following chart summarizes the forward and connect filter actions available for Restricted Bridging:

Filter Action	*Distribution List*	*Result*
FORWARD	LAN	A packet matching this filter will only be forwarded on the LAN ports. The packet will not be sent to any remote sites connected over the WAN.
FORWARD	WAN	A packet matching this filter will only be forwarded to remote sites connected on the WAN. The packet will not be sent to the LAN ports.
FORWARD	ALL	A packet matching this filter will be forwarded on the LAN ports and forwarded to remote sites connected over the WAN.
FORWARD	Device List*	A packet matching this filter will only be forwarded to the specified Device List.
CONNECT	Device List*	A packet matching this filter will be connected to the specified Device List.

For Restricted Bridging, the following additional filter actions are available only on a system with an Ethernet-2 adapter executing the local bridge option:

Filter Action	*Distribution List*	*Result*
FORWARD	LAN PORT 1	A packet matching this filter will only be forwarded on LAN port 1. The packet will not be sent to remote sites connected over the WAN or to LAN port 2.
FORWARD	LAN PORT 2	A packet matching this filter will only be forwarded on LAN port 2. The packet will not be sent to remote sites connected over the WAN or to LAN port 1.
FORWARD	LAN PORT 1 and WAN	A packet matching this filter will only be sent to remote sites connected over the WAN and to LAN port 1. The packet will not be forwarded on LAN port 2.
FORWARD	LAN PORT 2 and WAN	A packet matching this filter will only be sent to remote sites connected over the WAN and to LAN port 2. The packet will not be forwarded on LAN port 1.
FORWARD	Device List*	A packet matching this filter will only be sent to the specified Device List.
CONNECT	Device List*	A packet matching this filter will be connected to the specified Device List.

It is possible to use a discard filter action to selectively discard packets that have been forwarded through the previous restricted bridging forwarding filters. The following chart summarizes the discard filter actions available for Restricted Bridging:

Filter Action	*Distribution List*	*Result*
DISCARD	LAN	A packet matching this filter will be discarded on the LAN ports. The packet will be sent to all remote sites connected over the WAN.
DISCARD	WAN	A packet matching this filter will be discarded to remote sites connected on the WAN. The packet will be sent to the LAN ports.
DISCARD	ALL	A packet matching this filter will be discarded on the LAN ports and WAN ports.
DISCARD	Device List*	A packet matching this filter will not be sent to the specified Device List.

* *Device List* may be the on-node device database, or it may be located on an off-node authentication server.

For Restricted Bridging, the following additional discard filter actions are available only on a system with an Ethernet-2 adapter executing the local bridge option:

Filter Action	*Distribution List*	*Result*
DISCARD	LAN PORT 1	A packet matching this filter will be discarded on LAN port 1. The packet will be sent to remote sites connected over the WAN or to LAN port 2.
DISCARD	LAN PORT 2	A packet matching this filter will be forwarded on LAN port 2. The packet will not be sent to remote sites connected over the WAN or to LAN port 1.
DISCARD	LAN PORT 1 and WAN	A packet matching this filter will not be sent to remote sites connected over the WAN and to LAN port 1. The packet will be forwarded on LAN port 2.
DISCARD	LAN PORT 2 and WAN	A packet matching this filter will not be sent to remote sites connected over the WAN and to LAN port 2. The packet will be forwarded on LAN port 1.
DISCARD	Device List*	A packet matching this filter will not be sent to the specified Device List.

* *Device List* may be the on-node device database, or it may be located on an off-node authentication server.

DIAL OUT USING BRIDGE FILTERS

Each type of bridge filter for each operating mode supports a different set of "forwarding actions." Your particular set up and device configuration will determine which type of filter and forwarding arrangement will be the most useful. For our purposes, we will illustrate what we feel to be the most commonly used filter arrangement: the Destination MAC Address Filter used in Unrestricted Mode.

EXAMPLE: BRIDGE DIAL OUT USING A DESTINATION MAC ADDRESS FILTER

Consider the following situation: you know the destination of a packet, and you want to control its forwarding action. With the use of filters, you can:

- specify a Device List for connection
- specify a Device List for which you would discard the packet
- specify a LAN or WAN for which you would discard the packet
- specify a complete discard of the packet for the entire system

The following example illustrates how to configure a filter when you know the Destination MAC Address. To configure filters in other situations, follow similar principles as you work your way through the CFGEDIT screens. For details on the differences between filters and their forwarding actions, refer to the discussion beginning on page 274.

Preliminaries

Be sure your system's resources are properly configured. This includes resources, lines and datalinks, if applicable. Refer to the chapter *Configuring Resources and Lines* for details.

In order to have the CyberSWITCH successfully dial out, you must have the device information properly set up and the dial out number stipulated. Instructions for configuring on-node device entries are included in the section *Configuring a On-node Device Database* in the *Configuring Device Level Databases* chapter.

In order to use the remote bridge feature and properly set up filters, you must:

- enable MAC layer bridging
- select your mode of operation (restricted or unrestricted)

Access these configuration elements through CFGEDIT's Options Menu, Configure Bridging. For our example, we will use the Unrestricted Mode for our Mode of Operation.

Configuring a Destination MAC Address Filter

To configure a bridge filter, you must advance through CFGEDIT's menus to the Bridge Menu. To do this:

1. From CFGEDIT's Main Menu, select *Options*.

2. From the Options Menu, select *Bridging*.

3. From the Bridging Menu, select *Bridge Filters*. The menus similar to the following will then be displayed. Follow the item selection process shown in the screens (the selections are in bold).

```
Bridge Filter Menu:

   1) Protocol Definition
   2) Source MAC Address Filter
   3) Destination MAC Address Filter
   4) Protocol Filter
   5) Packet Data Filter

Select function from above or <RET> for previous menu: 3
```

```
Current Destination Address Filter:

id   DEST ADDRESS     ACTION           DISTRIBUTION LIST
-----------------------------------------------------

There are currently no Destination Address Filters configured.

1) to Add a Destination Address Filter or press <RET> for previous menu: 1
```

```
Destination MAC Address? 112233445566

   1) DISCARD
   2) CONNECT

Forward Action from the above list?
```

If you choose CONNECT as a forwarding action, the system will connect and forward the packet to the specified device list only. This eliminates the need for the packet to be broadcast to all connections. After specifying the "connect," you are prompted for the device name:

```
DEVICE LIST For CONNECT Filter

Device Name
----------------------

1) to Add a Device or press <RET> for previous menu: 1

Enter Device Name or <RET> to cancel? John
```

```
DEVICE LIST For CONNECT Filter

id Device Name
-- ------------------
(1) John


(1) Add, (2) Change, (3) Delete a Device or press <RET> for previous menu?   <RET>
```

```
Current Destination Address Filter Configuration:

id   DEST ADDRESS     ACTION          DISTRIBUTION LIST
-------------------------------------------------------
1    112233445566     CONNECT         John

(1) Add, (2) Change, (3) Delete a Destination Address Filter or <RET> to return to
the previous menu?
```

Your filter is now configured for this example. Remember, each type of filter for each operating mode supports a different set of "forwarding actions." These are described in detail earlier in the *Bridge Filters* section.

KNOWN CONNECT LIST

The Known Connect List is a configurable list of all devices for which you want the system to connect and forward bridged packets.

CONFIGURING THE KNOWN CONNECT LIST

Notes: Before beginning, be sure your system's resources are properly configured. This includes resources, lines, and datalinks, if applicable. Refer to the *Configuring Resources and Lines* chapter.

In order to successfully dial out to a device on the CyberSWITCH's Known Connect List, you must have the device information properly set up and the dial-out number(s) stipulated. Refer to the *On-node Device Database* section found in the *Configuring Device Level Databases* chapter.

The dial out call must be made within a configured amount of time from its last connection. This time is configurable through the Bridge Configuration menu's Spanning Tree Parameters. The parameter for configuring the time is called the bridge age time. The default bridge age time is 5 minutes. Refer to page 266 for instructions on changing the default value.

USING CFGEDIT

1. From the Bridging Menu press (5) to configure the Known Connect List. The following screen will then be displayed:

```
DEVICE LIST For CONNECT Filter

Device Name
----------------------

1) to Add a Device or press <RET> for previous menu? 1

Enter 1) to add a Device Name or <RET> to previous menu:
```

2. Press (1) to add a device to the Known Connect List.

3. Repeat step 2 for all devices you want included on this list.

KNOWN CONNECT LIST CONFIGURATION ELEMENTS

DEVICE NAME
The name of a bridge device that has been preconfigured in the *On-node Device Database* section of the *Configuring Device Level Databases* chapter. This is a device to which you want the system to connect and forward bridged unicast packets.

KNOWN CONNECT LIST BACKGROUND INFORMATION

In Unrestricted Mode, standard bridge processing attempts to forward frames with unknown or broadcast MAC addresses through all available interfaces. This can cause a problem with the limited bandwidth and high cost of dial-up WAN links. The CyberSWITCH's Known Connect List feature, and its support of bridge filters, gives you flexible options in controlling the risk of bridge flooding over WAN links.

When operating as a bridge or in IP Host Mode, in the course of processing the MAC frames, the CyberSWITCH builds its bridge table and associates each MAC address it sees with an interface. When a remote bridge establishes a connection and begins sending traffic to the CyberSWITCH, the CyberSWITCH adds these remote addresses to its bridge table and associates the remote bridge with them. Later, if the connection is dropped, and if the CyberSWITCH receives a packet destined for one of the remote addresses, it will re-establish the connection with the remote bridge *only if* the remote bridge is specified on the Known Connect List, *or if* a forwarding filter is configured. Furthermore, if the Known Connect List option is used, the CyberSWITCH can only re-establish the connection while the remote bridge is still "known"; that is, if the system receives the new, outbound packet before the Spanning Tree Bridge Age Time timer ages-out the destination MAC address from the bridge table. If a connect filter is used, the CyberSWITCH can re-establish the connection regardless of how long it's been since the last connection. The default Bridge Age Time is 5 minutes. Refer to page 266 to change the default value.

CONFIGURING ADVANCED IP ROUTING

OVERVIEW

By default, IP routing is disabled when you first install your system software. After IP routing is enabled, there are optional advanced features available. Optional advanced IP routing features include:

- Static ARP Table Entries
  ARP (Address Resolution Protocol) is used to translate IP addresses to Ethernet addresses. As a rule, this translation is handled dynamically. In rare situations, a user may need to manually enter this translation. This menu item allows you enter a static ARP table entry manually.
- Enable / Disable Isolated Mode Option
  The Isolated mode option helps to restrict the resources to which remote IP devices can get access.
- Static Routes Lookup via RADIUS
  The Static Routes Lookup via Radius option allows you to either enable or disable maintaining static routes for devices on the RADIUS Server. This option is only applicable when a RADIUS Server is in use.
- IP Address Pool
  The IP Address Pool allows you to configure a list of IP addresses that can be dynamically assigned to remote IP devices as they connect to the system.
- IP Filters
  IP Filters allow you to control the admission and transmission of individual IP datagrams based on the datagram's contents.
- DHCP
  Dynamic Host Configuration Protocol (DHCP) allows you to access the DHCP server to allocate IP addresses to all types of remote IP devices.
- Security Associations
  If you have purchased the CyberSWITCH encryption option, you will need to configure a set of Security Associations in order to use IP layer encryption. These associations include the IP addresses of datagrams that you select to be encrypted.
- NBNS and DNS Name Server Addresses
  This feature allows you to assign IP addresses to Domain Name System (DNS) or NetBIOS Name Servers (NBNS).

This chapter includes a section for each advanced IP routing feature.

STATIC ARP TABLE ENTRIES

CONFIGURING STATIC ARP TABLE ENTRIES

USING CFGEDIT

Once IP has been enabled, the full IP Configuration menu will be displayed as shown below:

```
IP Routing Menu:

   1)  IP Routing (Enable/Disable)
   2)  IP Operating Mode
   3)  IP Interfaces
   4)  IP Static Routes
   5)  RIP (Enable/Disable)
   6)  IP Static ARP Table Entries
   7)  Isolated mode (Enable/Disable)
   8)  Static Route Lookup via RADIUS (Enable/Disable)
   9)  IP Address Pool
   10) DHCP Configuration
   11) IP Filters
   12) NBNS and DNS name server addresses
   13) Security Associations

Select function from above or <RET> for previous menu:
```

The advanced IP routing options, including ARP table entries, are configured through this menu. To enter a static ARP table entry manually:

1. Select *Static ARP Table Entries* from the IP menu.

2. Select to add a Static ARP table entry.

3. Enter the device's IP address.

4. Enter the device's MAC address.

STATIC ARP TABLE ENTRIES CONFIGURATION ELEMENTS

IP ADDRESS
The IP address for the device for which you are making an entry. Only LAN interfaces are valid.

MAC ADDRESS
The MAC address (Ethernet address) for the device for which you are making an entry.

STATIC ARP TABLE ENTRIES BACKGROUND INFORMATION

When sending out IP packets, ARP (Address Resolution Protocol) is used to translate IP addresses to Ethernet addresses. As a rule, this translation is done dynamically. In rare situations, you may need to manually enter a static ARP table entry. Maximum configuration allowed: 16 static ARP entries. Use the `ip arp` command to display all dynamic or statically configured ARP entries.

Note: Static ARP entries can be created only for LAN interfaces. They are not supported for WAN RLAN interfaces.

THE ISOLATED MODE

CONFIGURING THE ISOLATED MODE

USING CFGEDIT

1. Select *Isolated Mode (Enable/Disable)* from the IP menu.

2. Follow the onscreen instructions to either enable or disable the isolated mode.

ISOLATED MODE CONFIGURATION ELEMENTS

ISOLATED MODE STATUS
You may enable or disable the Isolated Mode option.

ISOLATED MODE BACKGROUND INFORMATION

When operating with isolated mode enabled, the CyberSWITCH does not relay IP datagrams received from the WAN to other IP routers / hosts located on the WAN. IP datagrams received from the WAN will be discarded if they need to be forwarded over the WAN. IP datagrams received on the LAN interface are forwarded to each required interface.

WAN-to-LAN and LAN-to-LAN routing still works if Isolated Mode is enabled.

STATIC ROUTE LOOKUP VIA RADIUS

Note: This option is only applicable when a RADIUS Server is in use.

CONFIGURING STATIC ROUTE LOOKUP VIA RADIUS

USING CFGEDIT

1. Select *Static Route Lookup via RADIUS (Enable/Disable)* from the IP menu.

2. Follow the onscreen instructions to either enable or disable this feature.

USING MANAGE MODE

`ipradius`
Displays the current enabled status of the IP route lookup via RADIUS feature.

`ipradius off`
Disables the lookup of IP routes lookup via RADIUS.

`ipradius on`
Enables the lookup of IP routes lookup via RADIUS.

STATIC ROUTE VIA RADIUS CONFIGURATION ELEMENTS

STATIC ROUTE VIA RADIUS STATUS
You may enable or disable this option.

STATIC ROUTE LOOKUP VIA RADIUS BACKGROUND INFORMATION

The Static Routes Lookup via RADIUS option allows you to maintain static routes for devices on the RADIUS Server. When there are multiple CyberSWITCHes at one site, the IP static routes information needs to be duplicated on all systems. The Static Route Lookup via RADIUS feature allows you to maintain all of the IP static routes information for multiple systems on the RADIUS server by enabling this feature. The systems will download necessary static routes information from the server when needed.

Refer to this guide's RADIUS configuration information. *The RADIUS Authentication Server User's Guide* (an electronic document) also provides information on the RADIUS Authentication Server. Refer to *Configuring the RADIUS Server* for instructions on obtaining this document.

IP ADDRESS POOL

CONFIGURING AN IP ADDRESS POOL

USING CFGEDIT

1. Select *IP Address Pool* from the IP menu.

2. Select to add an IP address.

3. If you are adding a single IP address:
   a. Enter the IP address.
   b. When prompted to enter the ending IP address press <return>.

4. If you are adding a range of IP addresses:
   a. Enter the first IP address in the range.
   b. Enter the ending IP address in the range.

   Note: A range of IP addresses can cover the associated interface IP address; however, this interface address will not be added to the IP address pool.

5. To delete a single IP address contained in a configured range:
   a. Select to delete an IP address.
   b. Select the Id of the range you want to delete the address from.
   c. Select to delete a single IP address contained in the range.
   d. Enter the IP address you would like to delete from the range.

IP ADDRESS POOL CONFIGURATION ELEMENTS

IP ADDRESS
This can be a single IP address, or a range of IP addresses that can be dynamically assigned to remote IP devices as they connect to the system.

IP ADDRESS POOL BACKGROUND INFORMATION

The IP Address Pool feature allows you to configure a list of IP addresses that can be dynamically assigned to remote IP devices as they connect to the system. This would occur if a remote IP device calls in to the system and has no IP address, and requests to have one assigned. With this capability, you no longer need to assign permanent IP addresses to all possible remote IP devices, but rather only as many IP addresses as the number of possible ISDN connections. If multiple connections are used, you would not need as many IP addresses as the number of possible ISDN connections. This can result in a reduction of the number of IP addresses required for remote IP devices.

When a PPP connection is established to the system, the system and the remote device exchange their IP addresses during the IPCP (IP Control Protocol) phase. If the remote device does not know its own IP address, the system will assign a proper IP address to it. A proper IP address can be a permanent IP address configured for the remote device in the device table, or it can be one of the IP addresses configured in the IP Address Pool. If an IP address from the address pool is used, it will be returned to the pool when the connection is terminated. This allows the IP address to be reused for other remote IP devices. As many as 64 IP addresses can be configured in the IP Address Pool.

Notes: Dynamic IP address assignment from the IP Address Pool is only supported via PPP IPCP.

An IP address should not be configured for the device (either in the on-node device database or in a remote authentication database) if an IP address is to be assigned to the device from the IP address pool.

IP FILTERS

The IP Filter Configuration is a three-part process. It involves:

1. configuring packet types
2. configuring the filters to act on these packet types
3. applying the filters to selected points in the IP packet processing path

We suggest you become familiar with the IP Filtering mechanism before attempting a configuration. Refer to *IP Filters Background Information*.

Understandably, when IP Filters are enabled, system performance will slow down. This is due to the fact that every IP packet will experience a delay while the system is searching for a filter match. System performance will also be affected by the number of packets, conditions and filters configured. Refer to the *Limitations* section for details.

INITIATING THE IP FILTER CONFIGURATION

USING CFGEDIT

To begin the configuration process, IP must be enabled. Access IP Filter configuration through the extended IP Routing Menu:

```
IP Routing Menu:

   1)  IP Routing (Enable/Disable)
   2)  IP Operating Mode
   3)  IP Interfaces
   4)  IP Static Routes
   5)  RIP (Enable/Disable)
   6)  IP Static ARP Table Entries
   7)  Isolated Mode(Enable/Disable)
   8)  Static Route Lookup via RADIUS(Enable/Disable)
   9)  IP Address Pool
   10) DHCP Configuration
   11) IP Filter Information.

Select function from above or <RET> for previous menu: 11
```

Upon selecting IP Filter Information, the following sub-menu is displayed:

```
IP Filters:

   1)  Packet Types
   2)  Forwarding Filters
   3)  Connection Filter
   4)  Exception Filter
   5)  Apply Global Forwarding Filter.

Select function from above or <RET> for previous menu:
```

The configuration of each of the listed functions is described in the following discussion.

USING MANAGE MODE

ipfilt

This command displays the *IP Filter Configuration* screen from which you can set up your packet types and filters.

Note: Since IP Network Interfaces are not currently changeable within Manage Mode, the *application* of filters to Interfaces may only be performed within CFGEDIT.

CONFIGURING PACKET TYPES

USING CFGEDIT

1. Select *Packet Types* from the IP Filter menu.

2. Select *Add*.
3. Assign a unique name to the packet type. The system will then display the new packet with wild card values, similar to the following:

```
Current Configuration for PACKET TYPE "Type_One"

1) IP Source Address                  AND 0.0.0.0 EQUAL 0.0.0.0
2) IP Destination Address             AND 0.0.0.0 EQUAL 0.0.0.0
3) IP Protocol                        EQ ANY

Select function from above or <RET> for previous menu:
```

The screen identifies the common portion of the packet type, which includes the IP addresses and protocol information. To modify these values, refer to the following section entitled *Configuring the Common IP Portion*.

The criteria for IP addresses includes the:
- *mask* (logically ANDed with the packet's address field),
- *target value* (with which the result of the AND operation is compared), and
- *operator* (which specifies the type of comparison to perform)

Based upon what you select for IP protocol, you will be prompted for additional information, as described in following sections. The IP protocol item allows packet matching based upon one of the following:
- a set of recognized upper-level protocols
- a wild card value (with wild card valid only with an "EQUAL" operator), or
- an arbitrary numeric value

The upper-level protocols include:
- TCP
- UDP
- ICPM

CONFIGURING THE COMMON IP PORTION

USING CFGEDIT

1. To change the source address, select *IP Source Address* from the *PACKET TYPE* menu.

2. Provide IP address mask.

3. Provide comparison operator (equal or not equal).

4. Provide IP address target.

5. To change the destination address, select *IP Destination Address* from the *PACKET TYPE* menu. Continue with steps two through 4, as just described.

6. From the *PACKET TYPE* menu, select *IP Protocol.*

7. Select Comparison Operator.
   - *If you select EQUAL,* you may choose between a specific upper-level protocol, an arbitrary numeric value, or "any" protocol.
   - *If you select NOT EQUAL,* you may choose between a specific upper-level protocol or an arbitrary numeric value only.

8. Select IP protocol. If you choose an upper-level protocol, refer to the three following configuration sections: *Configuring TCP*, *Configuring UDP*, and *Configuring ICMP*.

CONFIGURING TCP

If you have selected TCP as your IP protocol, a screen similar to the following is displayed. Note that the following TCP defaults constitute a wild card match for any TCP packet:

```
PACKET TYPE "Type_One":

1) IP Source Address          AND 0.0.0.0 EQUAL 0.0.0.0
2) IP Destination Address     AND 0.0.0.0 EQUAL 0.0.0.0
3) IP Protocol                EQUAL TCP
4) TCP Source Port            RANGE 0 - 65535
5) TCP Destination Port       RANGE 0 - 65535
6) TCP Control                ANY

Select function from above or <RET> for previous menu:
```

1. Select *TCP Source Port*. Note that the ports are specified in terms of an operator.

2. Select a comparison operator.

3. *If you have chosen the comparison operator of "RANGE"*, you will be prompted for upper-range and lower-range values. *If you have chosen a comparison operator other than "RANGE"*, you will be prompted for a specific TCP port number.

4. Select *TCP Destination Port*. Note that the ports are specified in terms of an operator.

5. Select a comparison operator.

6. *If you have chosen the comparison operator of "RANGE"*, you will be prompted for upper-range and lower-range values. *If you have chosen a comparison operator other than "RANGE"*, you will be prompted for a specific TCP port number.

7. Select *TCP Control*.

8. Specify a control value (*any*, *established*, or *not established*).

CONFIGURING UDP

If you have selected UDP as your IP protocol, a screen similar to the following is displayed. Note that the following UDP defaults constitute a wild card match for any UDP packet:

```
PACKET TYPE "Type_One":

1) IP Source Address          AND 0.0.0.0 EQUAL 0.0.0.0
2) IP Destination Address     AND 0.0.0.0 EQUAL 0.0.0.0
3) IP Protocol                EQUAL UDP
4) UDP Source Port            RANGE 0 - 65535
5) UDP Destination Port       RANGE 0 - 65535

Id of the item to change, <RET> to accept changes or <CTRL-C> to cancel
```

1. Select *UDP Source Port*. Note that the ports are specified in terms of an operator.

2. Select a comparison operator.

3. *If you have chosen the comparison operator of "RANGE"*, you will be prompted for upper-range and lower-range values. *If you have chosen a comparison operator other than "RANGE"*, you will be prompted for a specific UDP port number.

4. Select *UDP Destination Port*. Note that the ports are specified in terms of an operator.

5. Select a comparison operator.

6. *If you have chosen the comparison operator of "RANGE"*, you will be prompted for upper-range and lower-range values. *If you have chosen a comparison operator other than "RANGE"*, you will be prompted for a specific UDP port number.

CONFIGURING ICMP

If you have selected ICMP as your IP protocol, a screen similar to the following is displayed. Note that the following ICMP defaults constitute a wild card match for any ICMP packet:

```
PACKET TYPE "Type_One":

1) IP Source Address        AND 0.0.0.0 EQUAL 0.0.0.0
2) IP Destination Address   AND 0.0.0.0 EQUAL 0.0.0.0
3) IP Protocol              EQUAL ICMP
4) ICMP Type                EQUAL ANY
5) ICMP Code                EQUAL ANY

Id of the item to change, <RET> to accept changes or <CTRL-C> to cancel
```

1. Select *ICMP Type*.

2. Select a comparison operator.

3. *If you choose "EQUAL"*, you may specify an ICMP type of "ANY", or you may specify a value. *If you choose "NOT EQUAL"*, you may only specify a numeric value for the ICMP type.

4. Select "ICMP Code".

5. Select a comparison operator.

6. *If you choose "EQUAL"*, you may specify an ICMP code of "ANY", or you may specify a numeric value. *If you choose "NOT EQUAL"*, you may only specify a numeric value for the ICMP code.

CONFIGURING FORWARDING FILTERS

The configuration of Forwarding Filters is a two-part process. First you must name the filter, and then you must create a list of conditions for the filter. To add a condition, you must name a previously-created packet type, and then name the action to perform on the specified packet type (i.e., *forward* or *discard*).

USING CFGEDIT

1. Select *Forwarding Filters* from the IP Filter menu.

2. Select *Add a Forwarding Filter*.

3. Provide a unique name for the filter you are creating. The *Conditions for Filter* menu is then displayed, similar to the following. (Note that the newly-created Forwarding Filter has a final condition of DISCARD as a default.)

```
Conditions for Filter "Filt_One"

Final Condition
               DISCARD        All Other Types

(1) Add,    (2) Change,    (3) Delete,    (4) Move a CONDITION,
(5) Change Default Condition   or press <RET> for previous menu?
```

4. Select *Add* to add a condition.

5. Enter the information for the condition:
   - name the previously-defined packet type
   - specify the action to take when an IP packet matches that type (*forward* or *discard*)

A screen similar to the following will then be displayed:

```
Conditions for Filter "Filt_One"

id
1              FORWARD        "Type_Two"

Final Condition
               DISCARD        All Other Types

(1) Add,    (2) Change,    (3) Delete,    (4) Move a CONDITION,
(5) Change Default Condition or <RET> to return to the previous menu?
```

6. *If the filter already has a forwarding condition (other than the final condition)*, an additional prompt is presented concerning the condition's position within the filter. Enter the location within the filter where the condition is to be added:
   - at the beginning
   - at the end
   - after the existing condition with id number "n".

Note: If the Final Condition of the filter needs modification, do so via the "Change Default Condition" selection on the "Conditions for Filter" menu. In this screen context, *default condition* refers to *final condition*.

CONFIGURING CONNECTION FILTERS

The IP Connection Filter is used at the point when an IP packet attempts to establish an outbound connection in order to continue the forwarding process. Its configuration parallels that of forwarding filters.

USING CFGEDIT

1. Select *Connection Filter* from the IP Filter menu.

2. Enable the Connection Filter. (By default, the Connection Filter is disabled.)

3. Select *Edit the Connection Filter*. A screen similar to the following will be displayed:

```
Conditions for "Connect_Filter"

Final Condition
               DISCARD        All Other Types

(1) Add,    (2) Change,    (3) Delete,    (4) Move a CONDITION,
(5) Change Default Condition   or press <RET> for previous menu?
```

4. Select *Add* to add a condition.

5. Enter the name of the packet type to be forwarded. A screen similar to the following is then displayed:

```
Conditions for "Connect_Filter"

id
1              FORWARD        "Type_Two"

Final Condition
               DISCARD        All Other Types

(1) Add,    (2) Change,    (3) Delete,    (4) Move a CONDITION,
(5) Change Default Condition   or press <RET> for previous menu?
```

6. *If the filter already has a forwarding condition (other than the final condition)*, an additional prompt is presented concerning the condition's position within the filter. Enter the location within the filter where the condition is to be added:
   - at the beginning
   - at the end
   - after the existing condition with id number "n".

Note: If the Final Condition of the filter needs modification, do so via the *Default Condition* selection on the *Conditions for Filter* menu. In this screen context, *default condition* refers to *final condition*.

CONFIGURING EXCEPTION FILTER

The IP Exception Filter is intended for temporary, special conditions within an existing forwarding filter. When enabled, it is logically appended to the beginning of each forwarding filter in effect.

USING CFGEDIT

1. Select *Exception Filter* from the IP Filter menu.

2. Enable the Exception Filter. (By default, the Exception Filter is disabled.)

3. Select *Edit the Exception Filter*. A screen similar to the following will be displayed:

```
Conditions for "Except_Filter"

Final Condition
               DISCARD        All Other Types

(1) Add,    (2) Change,    (3) Delete,    (4) Move a CONDITION,
(5) Change Default Condition   or press <RET> for previous menu:
```

4. Select *Add* to add a condition.

5. Enter the name of the packet type to be forwarded. A screen similar to the following is then displayed:

```
Conditions for "Except_Filter"

Final Condition
               DISCARD        All Other Types

(1) Add,    (2) Change,    (3) Delete,    (4) Move a CONDITION,
(5) Change Default Condition   or press <RET> for previous menu:
```

```
Conditions for "Except_Filter"

id
1              FORWARD        "Type_Two"

Final Condition
               DISCARD        All Other Types

(1) Add,    (2) Change,    (3) Delete,    (4) Move a CONDITION,
(5) Change Default Condition   or press <RET> for previous menu:
```

6. *If the filter already has a forwarding condition (other than the final condition)*, an additional prompt is presented concerning the condition's position within the filter. Enter the location within the filter where the condition is to be added:
   - at the beginning
   - at the end
   - after the existing condition with id number "n".

Note: If the Final Condition of the filter needs modification, do so via the *Change Default Condition* selection on the *Conditions for Filter* menu. In this screen context, *default condition* refers to *final condition*.

MODIFYING THE FINAL CONDITION FOR A FILTER

To change the final condition for a filter, select *Change Default Condition* (currently selection (5) on the *Conditions for Filter* menu.

APPLYING FILTERS

Once you have defined your forwarding filters, you must apply them to selected points in the IP routing process. There are three ways to apply filters:

- through a Network Interface
- globally
- on a per-user basis

APPLYING FILTERS TO NETWORK INTERFACES

1. Return to the *IP Configuration* menu (from *Options*).
2. Select *IP Interfaces*.
3. Select *Change*.
4. Select the interface on which the filter is to be applied.
5. Press <RET> until you reach the prompt which asks for *Input Filter Name*.
6. *If you want to apply an Input filter*, provide the filter name at the *Input Filter* prompt. If you do not want to apply an Input filter, press <RET>.
7. *If you want to apply an Output filter*, provide the filter name at the *Output Filter* prompt. If you do not want to apply an Output filter, press <RET>.

APPLYING THE GLOBAL FORWARDING FILTER

1. From the *IP Routing* menu, select *IP Filters.*
2. Select *Apply Global Forwarding Filter*.
3. Provide the global filter name.

APPLYING PER-DEVICE FORWARDING FILTERS

1. Return to the Main Menu.
2. Select *Security*.
3. Select *Device Level Databases*.
4. Select *On-node Device Entries.*
5. Select the device to which you want to apply the forwarding filter.

6. Select *IP Information*.

7. Select either *IP Input Filter* or *IP Output filter*.

8. Provide the filter name.

IP Filters Configuration Elements

The following elements are described in terms of the individual comparisons which make up the packet types. When an IP packet is subjected to a filter, the following comparisons are executed. The final result of the comparisons is a "match" if all comparisons are *true*, and a "no match" otherwise.

IP Addresses

These elements allow filtering based on the IP Addresses, which are expressed in two dotted decimal quantities, a Mask and a Target. The comparison entails the logical "AND" operation of the packet's IP Address and the specified Mask. The result of this operation is compared against the Target in either an EQUAL (EQ) or NOT EQUAL (NEQ) operation for determining if a match has occurred. The mask is used to create *wild card* or *don't care* conditions for the address comparison ('1' bits are significant and '0' bits are don't cares).

Examples:

0.0.0.0 EQ 0.0.0.0	Matches any IP address (wildcard and default).
255.255.255.0 EQ 128.131.23.0	If Class B network 128.131.0.0 is subnetted with 8 bits, this comparison matches any host on subnet 23.
255.255.255.0 NEQ 128.131.23.0	If Class B network 128.131.0.0 is subnetted with 8 bits, this comparison matches any host *except those* on subnet 23
255.255.255.255 EQ 128.131.23.59	Matches exactly the host 128.131.23.59
255.255.255.255 NEQ 128.131.23.59	Matches every host *except* 128.131.23.59

IP Protocol

This element applies a check to the Protocol field of the IP header using either an EQUAL or NOT EQUAL comparison. Symbolic mnemonics are supplied for the most popular upper level protocols (TCP, UDP, ICMP); when using an EQUAL comparison on these values, the corresponding protocol-specific comparisons are then enabled. A numeric value N (an unsigned quantity between 0 and 255) can be used for any other protocol without a specific mnemonic. "ANY" can also be specified as the protocol and is the default value, along with an EQUAL comparison, to yield the wild card value.

TCP and UDP Ports

These elements allow filtering based on the TCP Source and Destination Port fields, which are treated as 16 bit unsigned quantities (0-65535). These can be used to trap applications that have well-known port addresses, such as Telnet, FTP, etc. The packet's port value is compared to the value in the type using the specified operator:

EQ	equal to <port>
NEQ	not equal to <port>
LT	less than <port>
GT	greater than <port>
RANGE	inclusive range <port1> <= packet port value> = <port2>

Examples:

EQ 23: TCP port for the Telnet protocol.

RANGE 0 65535:Any TCP port (wild card and default).

TCP CONTROL

This element accesses the control bits of the TCP header, which are utilized to initiate and maintain the state of a TCP connection. "ANY" is the wild card and default value. TCP packets whose ACK or RST control bits are set will match the ESTABLISHED value, since they belong to an established connection. Conversely, a TCP packet which is attempting to open a new connection will carry neither of these bits and will match the NOT-ESTABLISHED value.

ICMP TYPE AND CODE

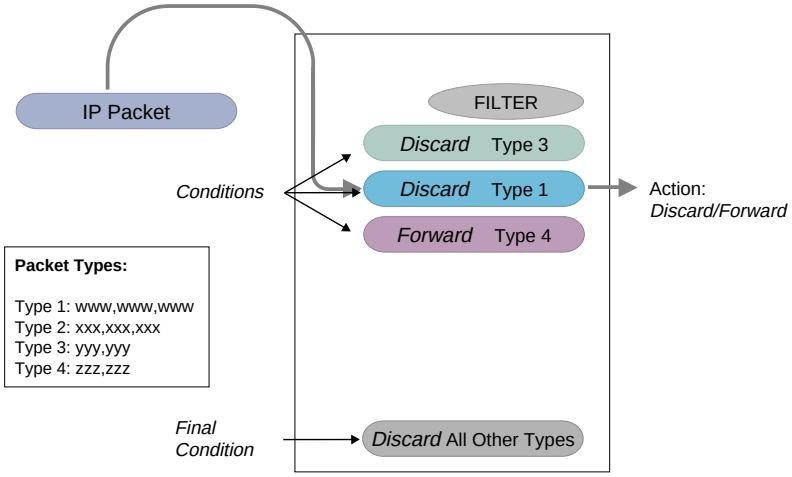
These fields allow filtering based on the specific function of an ICMP packet, via the Type and Code fields. Using an operator of EQUAL or NOT EQUAL, the packet's Type / Code is compared against the target values. These values may be a numeric quantity between 0 and 255; or the mnemonic "ANY" can be used with an EQUAL comparison as the wild card value.

IP FILTERS BACKGROUND INFORMATION

A *filter* is a list of conditions. It is the logical element which is applied to a point in the routing process to control packet flow. Each condition within a filter is created from one of the previously-defined packet types, along with the action to take when a packet matches that type.

IP Filters modify the normal processing flow of an IP packet as it passes through the various stages of IP Processing. When an IP packet encounters a filter, the filter's output - DISCARD or FORWARD - determines if the packet has permission to continue. There are two types of IP Filters. ***Forwarding Filters*** are selectively applied to the key locations in the IP routing process. The ***Connection Filter*** is applied to those datagrams which trigger a WAN connection in order to satisfy the forwarding process.

The following illustrates a packet that is passing through a filter. The packet is checked against each of the individual conditions of the filter before an action is performed:



Sample packet passing through a filter

FILTER COMPOSITION

The IP filtering mechanism is composed of three fundamental building blocks:

- *Packet Types*
  The criteria for describing an IP datagram's contents: IP Source and Destination Addresses, Protocol (TCP, UDP, etc.), Protocol-specific fields (TCP port, etc.). For example, Packet Types can be set up to specify such things as: "all packets arriving from IP Subnetwork X", "Telnet packets destined for host Y", or "All RIP packets". Packet Types are independently defined and may be referenced by multiple filters.

- ***Conditions***
  A Packet Type combined with an Action to take when a datagram matches that type. The Actions are DISCARD or FORWARD.

- ***Filter***
  An ordered list of Conditions. When an IP datagram passes through a filter, a sequential pass is made through the individual conditions. The first complete match of a Packet Type dictates the action which is applied to the datagram. When the action is DISCARD, the datagram is dropped. The filter also contains a configurable Final Condition which specifies the action to take if no match is found.

TYPES OF FILTERS

Forwarding Filters

A Forwarding Filter is a filter which forwards or discards specific packets according to whether these packets fulfill a list of defined conditions.Forwarding Filters may be applied to packets in one of the following ways:

- ***Globally***: independent of the packet's input or output path.
- through the ***Input* Network Interface**: applies the filter only to packets arriving on a specific

attached network.

- through the ***Output* Network Interface**: applies the filter only to packets which are transmitted on a specific attached network (i.e. after the Routing process has determined the next-hop network for the datagram).
- on a ***per-Device*** basis: applies a device-specific filter in addition to any Input or Output filters. This type of filtering is applicable only to WAN Network Interfaces.

Refer to the *Role of Filters* for more information on these filtering mechanisms.

Connection Filters

The Connection Filter, when enabled, is only applied when an IP datagram attempts to trigger a call on a WAN Output Interface. The initial default is that all such datagrams yield a FORWARD action, so the administrator must explicitly configure any desired connection restrictions. Note that the control offered by the IP Connection Filter is distinct from the "IP Callable" attribute of the Device Table. The IP Connection Filter permits connection control based on packet content, while the IP Callable feature applies such control based on the selected next hop.

Exception Filters

At certain times, you may want to allow specific IP packets to temporarily override the Forwarding Filters which have been applied. For example, you may want to allow temporary access to an authorized technical person via a path which is otherwise blocked via filters. One way to do this would be to simply make a temporary modification to the applicable filter or filters. However, the special concept of an *Exception Filter* is also expressly supported for this purpose.

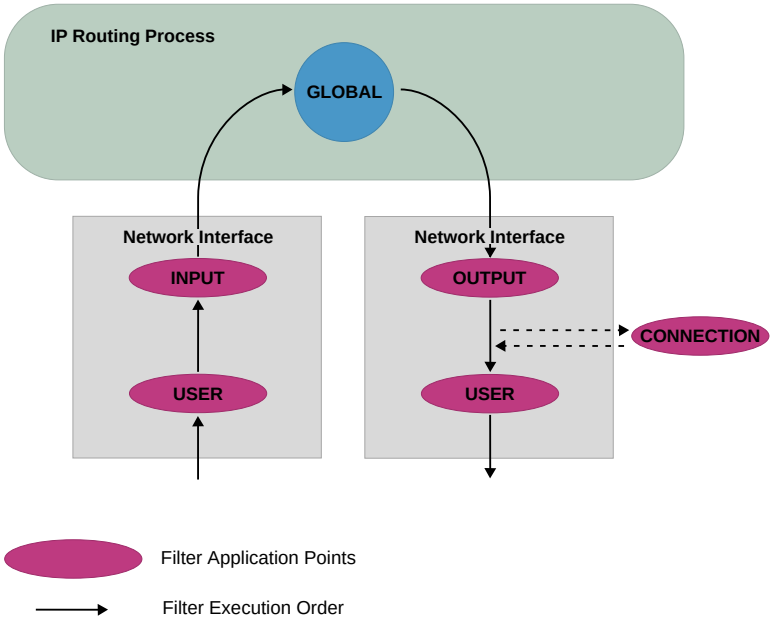
The Exception Filter is a built-in filter which is selectively enabled and disabled. When enabled, it is logically appended *before* each Forwarding Filter which an IP packet encounters. The makeup of the Exception Filter is identical to any other filter. Should a match occur, the specified action will be taken, effectively overriding the original filter. If no match occurs, the Exception Filter's Final action dictates the next processing step. When the Final action is FORWARD, filter execution flows into the original filter, thereby creating one logical filter. This is the default operation of the Exception Filter. The alternative for the no-match situation is a Final action of DISCARD, in which case the datagram is discarded.

Note: A final action of DISCARD in the Exception Filter will DISCARD all packets not matching the initial condition.

ROLE OF FILTERS IN THE IP PROCESSING FLOW

Refer to the following figure. It illustrates the exact order in which the filter application points are executed. Before reaching the IP routing process, incoming datagrams will first be subject to any User-specific filter (if arriving on a WAN interface) and secondly to any Input filter for the delivering Network Interface. Once a datagram has reached the IP routing process (either an incoming datagram or a datagram generated within the NE system), the Global filter, if enabled, is applied. When the routing process determines that a datagram is to be transmitted, that datagram is subject first to any Output filter of the selected to Network Interface. If the output interface is a WAN and it is necessary to first establish a connection, the Connection Filter, if enabled, is applied. Finally, any User-specific filter is applied (again, only if the datagram is being transmitted on WAN interface).

Because the Packet Types within the conditions specify both source and destination address information, Global application may often be sufficient to filter IP traffic across the entire system. However, the Input, Output and User-Based application points are defined in case the administrator needs to apply a finer level of filtering which cannot be obtained on a Global basis.



Example: order of execution of filter application points

Application to Network Interfaces

A forwarding filter is *applied to an IP Network Interface* through the IP Interface configuration. A filter may be applied to both the input and output stages of the Network Interface.

It is important to note that the Unnumbered WAN Interface which appears in the IP Interface configuration is simply the enabling condition for operation with unnumbered WAN links. The actual unnumbered Network Interfaces are created dynamically at run-time, with the name of the remote WAN device providing the unique identifier for the Interface. Consequently, when a filter is applied to the externally visible Unnumbered WAN Interface, it will apply to all dynamic unnumbered interfaces which are created internally at run-time. If it desired to apply a filter to a specific unnumbered interface, this can be accomplished by applying a User-Based filter.

PACKET TYPES

A Packet Type is a set of comparisons which are made against the contents of an IP packet. It is the fundamental element of an IP filter condition. For a match to occur, ALL the constituent comparisons must yield a TRUE result. The type is composed of a common packet portion which specifies fields in the IP header, and a protocol-specific portion which references the upper- layer protocol fields and is dependent upon which Protocol field of the IP Header, if any, is used as a criterion.

Common Portion:

IP Source Address	AND mmm.mmm.mmm.mmm EQ / NEQ ttt.ttt.ttt.ttt
IP Destination Address	AND mmm.mmm.mmm.mmm EQ / NEQ ttt.ttt.ttt.ttt
Protocol Field	EQ / NEQ TCP / UDP / ICMP / ANY / <n>

Protocol-Specific Portion *TCP*:

Source Port	EQ <port> / NEQ < port > / GT < port > / LT < port > / RANGE <p1> <p2>
Destination Port	EQ <port> / NEQ < port > / GT < port > / LT < port > / RANGE <p1> <p2>
Control	ANY / ESTABLISHED / NOT-ESTABLISHED

Protocol-Specific Portion, *UDP:*

Source Port	EQ <port> / NEQ < port > / GT < port > / LT < port > / RANGE <p1> <p2>
Destination Port	EQ <port> / NEQ < port > / GT < port > / LT < port > / RANGE <p1> <p2>

Protocol-Specific Portion, *ICMP:*

Type	EQ / NEQ n / ANY
Code	EQ / NEQ n / ANY

LIMITATIONS

System performance will be affected by the number of packets, conditions and filters configured. The more elements you have configured, the slower system performance. Refer to the following chart for the maximum number of elements supported:

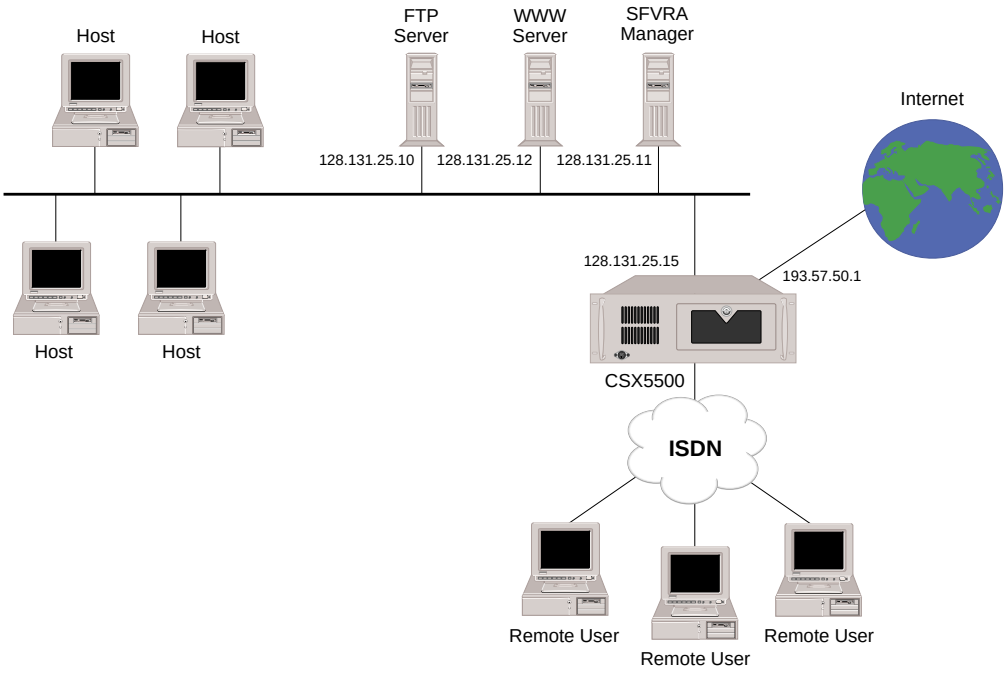
	Central Office Remote Access Switches	Work Group Remote Access Switches (single BRI port)
Maximum # Packet Types	1000	25
Maximum # Conditions	1000	25
Maximum # Filters	250	10

Note: If a packet is defined, it is counted toward the maximum number of packets allowed. Be aware that this applies even if:

- the packet is not used in a condition, and
- the filter is not enabled.

EXAMPLE OF AN IP FILTER CONFIGURATION

This example provides a simple filtering scenario in which a corporate LAN utilizes a CyberSWITCH to provide WAN access to both dial-in devices as well as the global Internet. A Netserver resides on the LAN to provide configuration support for the CyberSWITCH. Also on the LAN are an anonymous FTP server and a WWW server.



The following are the requirements/restrictions to be addressed by IP filters:

- No outside access allowed to the Netserver or the CyberSWITCH.
- The FTP and WWW servers must be accessible from anywhere.
- Corporate hosts (including dial-in devices) may initiate TCP-based sessions with the Internet, but not vice-versa. This covers the main IP applications such as TELNET, FTP, SMTP server and HTTP. An assumption for FTP is that the client program supports the "PASV" option, in which the data-transfer TCP connection is initiated by the client.
- No UDP traffic.

The interface to the Internet is via a numbered IP interface, which has the following filter applied to its Input stage. Using a final action of DISCARD, the strategy for the filter is to restrict everything but an explicitly permitted set of traffic.

FORWARD	IP Src 0.0.0.0, 0.0.0.0 IP Dst: 255.255.255.255, 128.131.25.10 IP Prot: ANY	Permits any host to access the FTP Server.
FORWARD	IP Src 0.0.0.0, 0.0.0.0 IP Dst: 255.255.255.255, 128.131.25.12 IP Prot: ANY	Permits any host to access the WWW Server
FORWARD	IP Src 0.0.0.0, 0.0.0.0 IP Dst: 0.0.0.0., 0.0.0.0 IP Prot: TCP TCP Src Port: RANGE 0 65535 TCP Dst Port: RANGE 0 65535 TCP Control: ESTABLISHED	Permits TCP traffic only from sessions which have already been initiated by corporate hosts.
FORWARD	IP Src 0.0.0.0, 0.0.0.0 IP Dst: 0.0.0.0., 0.0.0.0 IP Prot: ICMP	Permits all ICMP packets to enter (including ECHO packets for PING).
DISCARD	All other packet types	No-match action.

The corporate dial-in access is realized with a WAN Direct Interface, using a pool of IP addresses from the corporate LAN for dynamic assignment to the dial-in devices. These devices must first pass Authentication processing, so there is a level of security inherent on this interface that is not present on the Internet interface. Once authenticated, the devices are basically allowed to generate traffic in the same way that they can when operating from within the corporate LAN. This includes the ability to initiate TCP connections to the external Internet. Correspondingly, the strategy for this filter is different. Its purpose is to enforce the stated requirement of not allowing any external access to the Netserver or the CyberSWITCH itself.

DISCARD	IP Src 0.0.0.0, 0.0.0.0 IP Dst: 255.255.255.255, 128.131.25.11 IP Prot: ANY	Denies access to the Netserver.
DISCARD	IP Src 0.0.0.0, 0.0.0.0 IP Dst: 255.255.255.255, 128.131.25.15 IP Prot: ANY	Denies access to the CyberSWITCH itself.
DISCARD	IP Src 0.0.0.0, 0.0.0.0 IP Dst: 255.255.255.255, 193.57.50.1 IP Prot: ANY	Denies access to the CyberSWITCH itself.
FORWARD	All other packet types	No-match action

Now suppose that a situation arises in which it is temporarily necessary to allow remote access to the Netserver (for example, reconfiguration by a qualified member of staff who is offsite). Using the IP Address from which the temporary access will take place, this can be accomplished by enabling the Exception Filter. When traffic arrives from the Internet, the Exception filter will be executed first, thereby allowing an override of the existing conditions of the Input filter. The Exception filter would be set up as follows (the remote access is originated from address 201.55.89.100).

FORWARD	IP Src 255.255.255.255, 201.55.89.100 IP Dst: 255.255.255.255, 128.131.25.11 IP Prot: ANY	Allows specific host to access the Net-server.
FORWARD	All other packet types	If no match, let filter execution continue with the existing input filter.

Once the offsite maintenance is completed, the Exception filter would be disabled. Configuration control over the Exception filter is available both through CFGEDIT and Manage Mode (with Manage Mode being the most practical method due to its dynamic nature).

DHCP RELAY AGENT

CONFIGURING A DHCP RELAY AGENT

USING CFGEDIT

1. Select *DHCP Configuration* from the IP Routing menu.

2. Press 1 to begin the DHCP configuration.

3. Follow the onscreen instructions to enable the DHCP/BOOTP relay agent. Once the agent has been enabled, the following menu will be displayed:

```
DHCP/BOOTP Relay Agent Menu:

   1)  DHCP/BOOTP Relay Agent (Enable/Disable)
   2)  Relay Destination IP Addresses
   3)  Hop Count Threshold

Select function from above or <RET> for previous menu:
```

4. Press 2 to configure relay destination IP addresses.
   a. Press 1 to add an address.
   b. Enter the relay destination IP address in dotted decimal notation. If you want to broadcast out to find the DHCP server, enter 255.255.255.255 for the IP address.
   c. If you have entered 255.255.255.255 for the IP address, you will need to select the network interface to which DHCP/BOOTP request messages should be relayed.

5. Press 3 to configure the hop count threshold. Enter the threshold value, or press return to accept the default. Be careful when configuring the hop count. Make sure you have configured the threshold value high enough; messages with a hop field greater than this value will be discarded.

USING MANAGE MODE

dhcp
Displays the current DHCP configuration values.

dhcp change
Displays the same DHCP menu as CFGEDIT, allowing you to change the current DHCP configuration.

DHCP CONFIGURATION ELEMENTS

DHCP/BOOTP RELAY AGENT ENABLE/DISABLE FLAG

A global flag that indicates whether the system is relaying the DHCP/BOOTP BOOTREQUEST messages or not. The relay agent is disabled by default.

RELAY DESTINATION IP ADDRESSES

These are the IP addresses to which the system will relay BOOTREQUEST messages. For relay destinations which are broadcast/multicast IP addresses, the network interface to which the messages should be relayed also needs to be configured.

HOP COUNT THRESHOLD

This configuration element is used to limit the number of relay agents through which DHCP/BOOTP BOOTREQUEST messages can travel. BOOTREQUEST messages with a hops field value greater than this value will be discarded. The valid range is between 0 and 16, and the default is 4.

DHCP BACKGROUND INFORMATION

The DHCP/BOOTP Relay Agent feature provides a solution to the dynamic IP address assignment problems in the ISDN WAN environment. Those IP host devices with the DHCP client software that are connected to a central LAN through ISDN remote bridges are now able to obtain their IP addresses from a DHCP server located on a central LAN.

The Dynamic Host Configuration Protocol (DHCP) provides configuration parameters to IP host devices. DHCP consists of two components: a protocol for delivering host-specific configuration parameters (name servers, time servers and many more) from a DHCP server to a host; and a mechanism for allocation of network addresses to hosts. Since remote devices are not always on a main network (a corporate LAN, Internet), and there are only limited IP addresses available, it is desirable to assign the IP addresses to those devices only when they are connected to the main network. DHCP can be used to accomplish this task; and the DHCP/BOOTP Relay Agent helps DHCP work over WAN environments.

For more detailed DHCP/BOOTP information, refer to the following specifications:

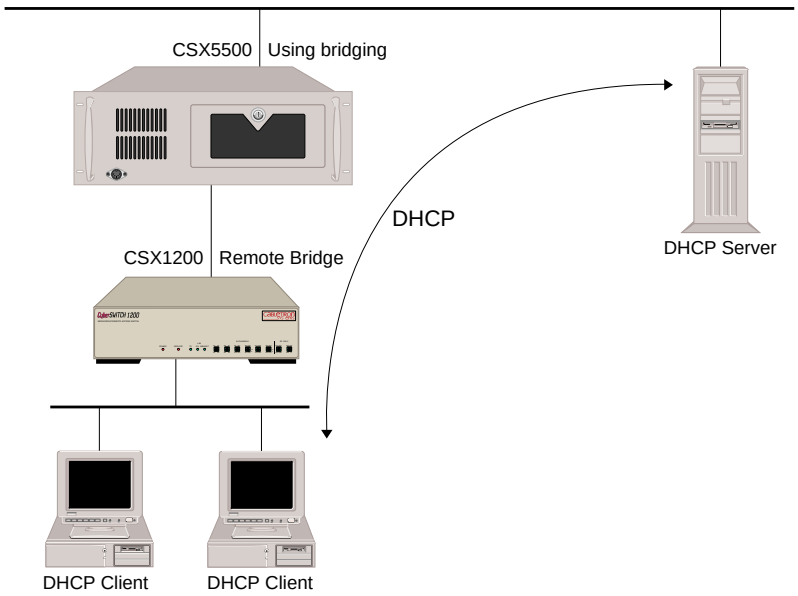
- RFC 1542: Clarifications and Extensions for the Bootstrap Protocol
- RFC 1541: Dynamic Host Configuration Protocol
- RFC 1534: Interoperation Between DHCP and BOOTP
- RFC 1533: DHCP Options and BOOTP Vendor Extensions

DHCP/BOOTP Relay Agent processing is extensively discussed in RFC 1542.

DHCP/BOOTP RELAY AGENT ENVIRONMENTS

The following sections describe the different environments in which the DHCP/BOOTP Relay Agent may be used.

Bridge to Bridge Environment

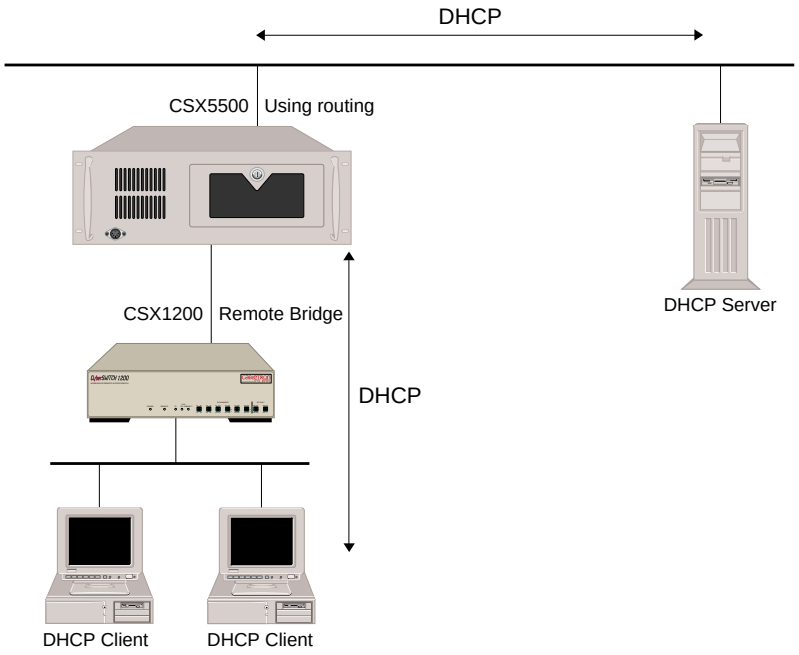


As shown in the picture above, when a remote LAN is connected with bridge devices, the DHCP server and clients communicate with each other as if they were on the same LAN. This is one example configuration of how DHCP can be used to accomplish the dynamic IP address assignment to the remote IP devices. (Note: This topology works without enabling any additional DHCP / BOOTP features.)

Router to Bridge Environment

Although the bridge to bridge environment is a simple way to deploy the dynamic IP address assignment using DHCP, it has some disadvantages. The major disadvantage is a broadcast storm. Since all remote LANs are connected through bridge devices, all broadcast traffic will be forwarded from one remote LAN to all the other LANs, and from a central LAN to all other remote LANs. This is especially undesirable in the environment where there are many remote LANs.

To solve this problem, IP routing should be turned on at the central site. Enabling routing at the central site will prevent the broadcast traffic from traveling all over the wide area network. Unfortunately, this also keeps DHCP messages from being exchanged, as they are transmitted in the broadcast packets. The DHCP Relay Agent resolves this situation, allowing only DHCP messages to be forwarded without letting all other broadcast traffic get through.

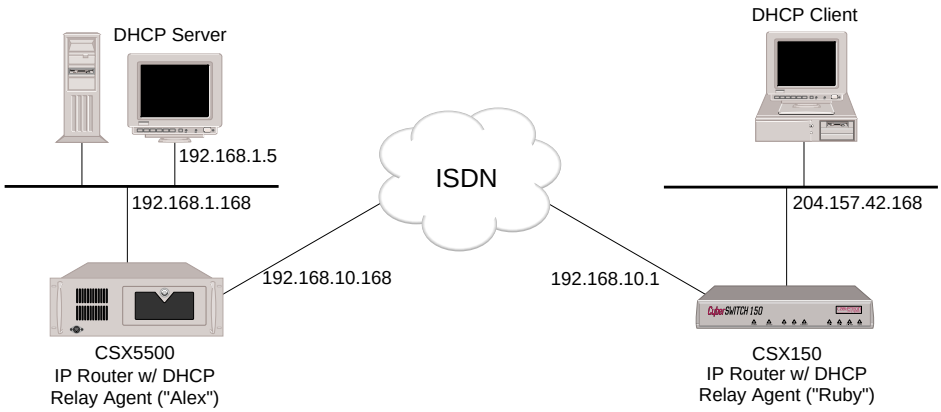


EXAMPLE DHCP CONFIGURATIONS

Below we have included two of the more common DHCP scenarios. These may help you configure your own DHCP feature.

IP Router to IP Router (with Relay Agents on both)

This configuration is useful when the “next hop” to the DHCP Server is another DHCP / BOOTP Relay Agent.



In this configuration, the DHCP Client is able to obtain its IP address from the DHCP Server (and any other information that the server provides), using the Relay Agents contained in both IP

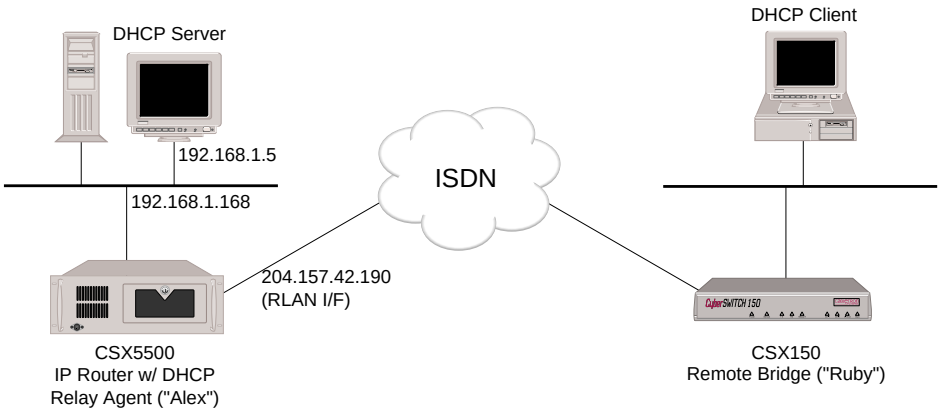
Routers shown in the diagram above. Sample configurations for the objects in the above network diagram are as follows:

Configuration for IP Router "Alex"	*Configuration for IP Router "Ruby"*
System Information: System Name = Alex System Password = stone	System Information: System Name = Ruby System Password = rubble
Security Level = Device Level (On-node Device Database, PAP security)	Security Level = Device Level (On-node Device Database, PAP security)
Bridging disabled	Bridging disabled
IP enabled (router mode) I/F = LAN (192.168.1.168) I/F = WAN (192.168.10.168) Static Route = (dest) 204.157.42.0 (next hop) 192.168.10.1	IP enabled (router mode) I/F = LAN (204.157.42.168) I/F = WAN (192.168.10.1)
DHCP enabled Relay Destination #1 = 192.168.1.5 (interface = "N/A") Hop Count Threshold = 4	DHCP enabled Relay Destination #1 = 192.168.10.168 (interface = "N/A") Hop Count Threshold = 4
Device = "Ruby" ISDN Line Protocol = PPP Dial Out Phone # = 5311 PAP Password = "rubble" IP Address = 192.168.10.1 IP Routing = enabled Make calls for IP data = enabled Bridging = disabled	Device = "Alex" ISDN Line Protocol = PPP Dial Out Phone # = 5411 PAP Password = "stone" IP Address = 192.168.10.168 IP Routing = enabled Make calls for IP data = enabled Bridging = disabled

Note: The DHCP Server must have a route specified to get back to the DHCP-enabled router Ruby, or use Alex as its default gateway.

Remote Bridge to IP Router (w/Relay Agent)

This configuration is useful when requests by a DHCP Client must be “bridged” to an IP Router that is also a DHCP / BOOTP Relay Agent. Our equipment is shown in this example, but any remote bridge device should work.



In this configuration, the DHCP Client is able to obtain its IP address from the DHCP Server (and any other information that the server provides), using the Relay Agent contained in the DHCP-enabled router “Alex.” “Ruby” is a remote bridge device which communicates with the IP router using a RLAN interface. Sample configurations for the objects in the above network diagram are:

Configuration for IP Router "Alex"	*Configuration for Remote Bridge "Ruby"*
System Information: System Name = Alex System Password = stone	System Information: System Name = Ruby System Password = rubble
Security Level = Device Level (On-node Device Database, PAP security)	Security Level = Device Level (On-node Device Database, PAP security)
Bridging disabled	Bridging enabled Bridge Packet Data Filter: offset=1; mask=00;value=00;action=CONNECT; dist list="Alex"
IP enabled (router mode) I/F = LAN (192.168.1.168) I/F = WAN RLAN (204.157.42.190)	IP disabled
DHCP enabled Relay Destination #1 = 192.168.1.5 (interface = "N/A") Hop Count Threshold = 4	DHCP disabled
Device = "Ruby" ISDN Line Protocol = PPP Dial Out Phone # = 5311 PAP Password = "rubble" IP Address = 204.157.42.0 IP Routing = disabled Bridging = enabled Make calls for Bridge data = disabled	Device = "Alex" ISDN Line Protocol = PPP Dial Out Phone # = 5411 PAP Password = "stone" IP Address = (none) IP Routing = disabled Bridging = enabled Make calls for Bridge data = enabled

Notes: The DHCP Server must have a route specified to get back to the DHCP-enabled router Alex, or use Alex as its default gateway.

When you are using a RLAN Interface, you are limited to one subnetwork.

DHCP PROXY CLIENT

CONFIGURING THE DHCP PROXY CLIENT

In order to configure the DHCP Proxy Client, you must first enable the client, and then configure client information for a WAN or a WAN (Direct Host) type interface.

USING CFGEDIT

1. Select *DHCP Configuration* from the IP menu.
2. Select *DHCP Proxy Client*.
3. Follow the onscreen instructions to enable the DHCP Proxy Client. Then return to the IP Routing Menu.
4. Select *IP Interfaces* from the IP Routing Menu.
5. Select *Add* to add a WAN or WAN (Direct Host) interface. Provide pertinent information in response to the prompts until you reach the DHCP Proxy Client Configuration submenu:

```
DHCP Proxy Client Configuration for this interface:

(1) Maximum number of IP addresses that can be obtained is 0.
(2) Number of IP addresses to pre-fetch is 0.
(3) LAN port to reach DHCP server on is 1.

Select function from above or <RET> for previous menu:
```

6. Select “1”. Enter the maximum number of IP addresses that may be obtained from a DHCP server for this interface.
7. Select “2”. Enter the number of IP addresses (obtained from DHCP servers) that should be available at all times for remote devices on this interface.
8. Select “3”. Enter the number of the LAN Port to use to reach a DHCP Server.
9. Press <RET> to display the newly-configured interface, and select “Y” (yes) to confirm its addition to the configuration.

USING MANAGE MODE

dhcp
Displays the current DHCP configuration values.

dhcp change
Displays the same DHCP menu as CFGEDIT, allowing you to change the current DHCP configuration.

DHCP Configuration Elements

DHCP Proxy Client Enable / Disable Flag
A global flag that indicates whether the DHCP Proxy Client feature is enabled or not. The proxy client is disabled by default.

Maximum Number of IP Addresses
Refers to the maximum number of IP addresses obtained from DHCP servers for this network interface. This number of IP addresses can be leased from DHCP servers for this interface and placed into the IP Address Pool. The range of this configuration value is 0 to "x" where "x" is the size of the Address Pool. The default for this value is 0.

Note: If all available entries in the IP Address Pool are assigned to one IP network interfaces's *maximum*, there will not be any more available for other interfaces. Therefore, take care to plan accordingly.

Number of IP Addresses to Pre-fetch
The configured number of IP addresses to have available at all times for an IP network interface. This means that the IP addresses have been placed in the IP Address Pool, but have not yet been leased to any remote devices. These IP addresses are sitting in the IP Address Pool waiting to be claimed by remote devices. The range of this configuration value is 0 to "x" where "x" is the maximum IP addresses to obtain for the IP network interface. The default for this value is 0.

LAN Port on which to reach the DHCP Server
This configuration value contains the number of the LAN port to use in order to reach a DHCP server. The range of this value is 1 to "x" where "x" is the number of configured LAN ports. The default for this value is 1.

DHCP Background Information

The DHCP Proxy Client feature enables the CyberSWITCH to dynamically obtain IP addresses from a DHCP server for IP host devices that support PPP. This feature compliments the *DHCP Relay Agent* feature, which supports remote bridges. Both features together allow the CyberSWITCH to access the DHCP server to allocate IP addresses to all types of remote IP devices, rather than maintaining separate IP address pools for separate devices.

Remote IP devices that use PPP to connect to the CyberSWITCH use PPP IPCP IP Address negotiation to dynamically obtain their IP addresses. In general, those devices are not capable of using DHCP to obtain the dynamic IP addresses. However, with the DCHP Proxy Client feature, the CyberSWITCH "pretends" to be a DHCP client. When a connection is established and a remote IP host device requests an IP address, the CyberSWITCH (acting as a DHCP client) obtains an IP address from the DHCP server. It then gives it to the remote device via IPCP.

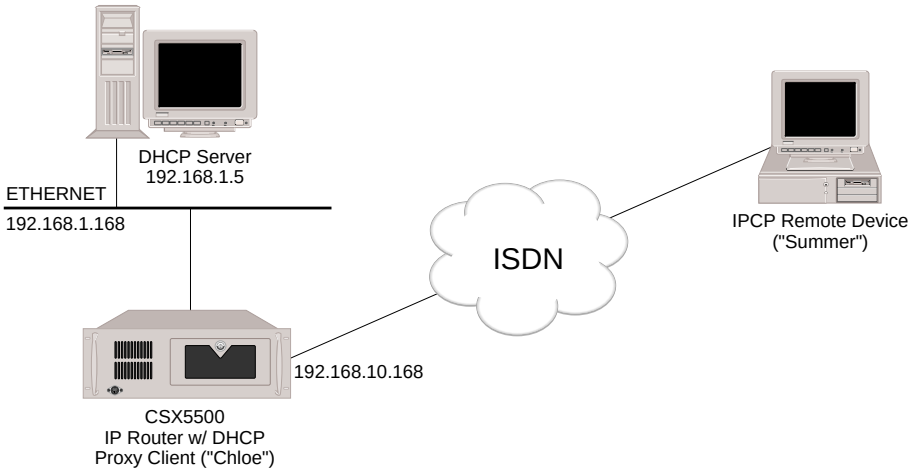
The CyberSWITCH is capable of prefetching some number of IP addresses so that connections can be established faster. You may configure two numbers for each WAN type network interface: the number of the IP addresses to prefetch ("x"), and the maximum number of IP addresses to obtain ("y"). The CyberSWITCH will prefetch "x" IP addresses for the network interface until it has obtained "y" addresses. For example, if the number to prefetch is 3, and the maximum number is 5, then 3 IP addresses will be prefetched immediately. As one IP address is assigned to a remote device, one IP address is obtained from a DHCP server until the total of 5 IP addresses have been obtained.

The DHCP Proxy Client feature is not applicable for the CyberSWITCH running in IP HOST mode.

DHCP servers must support use of the *broadcast bit* in order to obtain IP addresses for WAN (Direct Host) interfaces.

SAMPLE CONFIGURATION: IP ROUTER WITH DHCP PROXY CLIENT

The following illustrates a typical use of the DHCP Proxy Client. This configuration has the DHCP server and the CyberSWITCH located on the same LAN:



In this configuration, the remote IPCP device, “Summer”, is able to negotiate and obtain its IP address from the system’s IP Address Pool. IP addresses have been obtained from the DHCP server for the WAN interface 192.168.10.0. The following describes the configuration necessary for the CyberSWITCH (IP router) in the above diagram.

Configuration for IP Router "Chloe"
System Information: System Name = Chloe System Password =pets
Security Level = Device Level (On-node Device Database, PAP security)
Bridging disabled
IP enabled (router mode) I/F = LAN (192.168.1.168); LAN port 1 I/F = WAN explicit (192.168.10.168) DHCP related: max addrs to obtain=10 num addrs to pre-fetch=5 LAN port to reach server=1
DHCP configuration: Relay Agent disabled. Proxy Client enabled.
Device = "Summer" ISDN Line Protocol = PPP PAP Password = "dogs" IP Address = (none) IP Routing = enabled IP callable = disabled Bridging = disabled

SECURITY ASSOCIATIONS

The steps to configure security associations are merely listed here. For more detailed information, refer to *Configuring Encryption*.

CONFIGURING SECURITY ASSOCIATIONS

USING CFGEDIT

1. Select *Security Associations* from the IP Routing menu, and then select *Add*.
2. Select packet direction. You may choose *outgoing* (packets from trusted subnet to remote site), *incoming* (packets to trusted local subnet from a remote site), or *both*.
3. Enter the final destination IP address and subnet mask.
4. Enter the Source IP address and subnet mask.
5. Enter the destination gateway/IP address.
6. Enter an Initial Value (IV) length.
7. Enter Authentication Header information.
8. Enter the shared secret key.
9. Enter SPI information.

DNS AND NETBIOS ADDRESSES

CONFIGURING DNS AND NETBIOS ADDRESSES

USING CFGEDIT

1. From the CFGEDIT Main Menu, select *Options*.
2. Select *IP Routing*. If IP routing is disabled, enable this now.
3. Select *NBNS and DNS name server addresses*. A menu similar to the following will display:

```
Name Servers Menu:

   1) Primary Domain Name System server is not configured.
   2) Primary NetBIOS Name Server is 2.22.222.2
   3) Secondary Domain Name System server is 3.33.3.33
   4) Secondary NetBIOS Name Server is not configured.

Select name server to change or <RET> for previous menu: 1
```

4. Select the Name Server you wish to configure.
5. Provide the IP address of the Name Server that you have selected. The screen interaction will be similar to the following:

```
Enter the IP Address for the Primary Domain Name System server in dot-
ted decimal notation

Enter 0.0.0.0 to disable the Primary Domain Name System server
[default=0.0.0.0}?  1.22.33.44
```

```
Name Servers Menu:

   1) Primary Domain Name System server is 1.2.33.44.
   2) Primary NetBIOS Name Server is 2.22.222.2
   3) Secondary Domain Name System server is 3.33.3.33
   4) Secondary NetBIOS Name Server is not configured.

Select name server to change or <RET> for previous menu:  3

Enter the IP Address for the Secondary Domain Name System server in
dotted decimal notation

Enter 0.0.0.0 to disable the Primary Domain Name System server     [de-
fault=0.0.0.0}?  0.0.0.0
```

```
Name Servers Menu:

   1) Primary Domain Name System server is 1.2.33.44
   2) Primary NetBIOS Name Server is 2.22.222.2
   3) Secondary Domain Name System server is not configured.
   4) Secondary NetBIOS Name Server is not configured.

Select name server to change or <RET> for previous menu:  <RET>
```

USING MANAGE MODE

ipnamesv

This command displays the *Name Servers* menu from which you can enable, disable or change an IP address for a name server.

DNS/NBNS CONFIGURATION ELEMENTS

IP ADDRESS

The IP address(es) for the name server(s) you wish to configure. Your choices are:

- primary Domain Name System (DNS) server
- primary NetBIOS name server (NBNS)
- secondary Domain Name System (DNS) server
- secondary NetBIOS name server (NBNS)

DNS/NBNS BACKGROUND INFORMATION

This feature conforms to RFC 1877, which pertains to the negotiation of primary and secondary Domain Name System (DNS) and NetBIOS Name Server (NBNS) addresses. It is beneficial in an environment in which the CyberSWITCH is acting as a Network Service Provider. The feature allows clients that dial in to the CyberSWITCH to be assigned primary and secondary DNS and NBNS servers, if so defined on the CyberSWITCH.

CONFIGURING IPX

OVERVIEW

IPX protocol accepts data from remote devices and formats the data for transmission onto the network, and conversely, accepts data from the LAN and formats it so it can be understood by remote devices. In short, IPX allows remote devices and their servers to communicate.

The CyberSWITCH supports the standard method of routing datagrams over a network. The system provides bandwidth management features to make the interconnection of IPX networks cost effective over demand type connections like ISDN. Additional security features provide data privacy for networks using IPX that are connected by the system.

By default, IPX routing is disabled when you first install your system software. After IPX routing is enabled, the full IPX feature is available for configuration. The IPX configuration process includes:

- configuring the IPX internal network number
- configuring IPX interface information
- enabling / disabling routing protocols (RIP and SAP)
- configuring IPX static routes
- configuring NetWare static services
- configuring IPX spoofing information
- configuring IPX type 20 packet handling
- enabling / disabling the isolated mode
- configuring Triggered RIP / SAP
- configuring individual devices for IPX routing

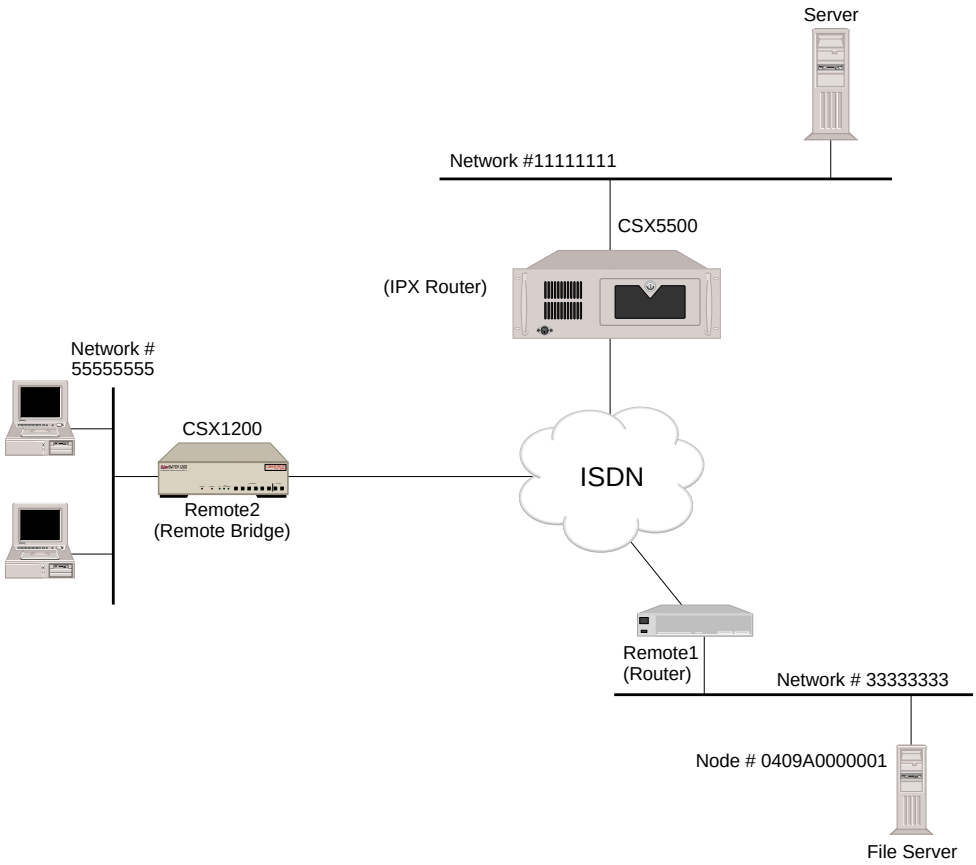
Notes: You must configure some type of network security in order to provide IPX routing over WAN connections.

In addition, with the availability of Triggered RIP / SAP, you most likely will not need to configure static routes and services. However, Cabletron still supports them. Situations may arise in which a remote router cannot implement Triggered RIP / SAP. In that case, you then have the option of configuring static routes and services.

CONFIGURING IPX INFORMATION

Note: IPX is available only if you have purchased the additional software module for our IPX feature.

To help you configure your IPX information, we have included an illustration of a sample network. As we explain the steps, we provide sample CFGEDIT screens. The screens include information from the sample network. You may find it helpful to refer to the graphic and to the sample screens for clarification while completing your IPX configuration.



	CSX5500	*Remote Router*	*CSX1200*
External Network Number	11111111	33333333	55555555
Internal Network Number	12F8	3A11	n/a

IPX ROUTING OPTION

ENABLING/DISABLING IPX

Note: The CyberSWITCH does not currently provide IPX data transfer over X.25 links.

USING CFGEDIT

1. Select *Options* from the main menu.

2. Select *IPX Routing* from the Options menu. The following menu will be displayed:

```
IPX Menu:

   1) IPX Routing (Enable/Disable)

Select function from above or <RET> for previous menu: 1

The IPX Routing feature is currently DISABLED.

Do you wish to ENABLE the IPX feature (Y or N) [default = N]? Y

The IPX Routing feature is currently ENABLED.

Press any key to continue.
```

3. As illustrated on the sample screen above, follow the onscreen instructions to enable IPX routing. The following extended IPX menu will be displayed:

```
IPX Menu:

   1)  IPX Routing (Enable/Disable)
   2)  IPX Internal Network number
   3)  IPX Interfaces
   4)  Routing Protocols (Enable/Disable)
   5)  IPX Static Routes
   6)  NetWare Static Services
   7)  IPX Spoofing Information
   8)  IPX Type 20 Protocol
   9)  Isolated mode (Enable/Disable)
   10) Triggered RIP/SAP

Select function from above or <RET> for previous menu:
```

You will use this menu to complete the IPX configuration.

IPX OPTION CONFIGURATION ELEMENT

STATUS

IPX can be either enabled or disabled, with disabled being the default. If the option is set to enable, the system will process and forward IPX data packets at the IPX network layer. If the option is set to disable, the system will process and forward IPX data packets at the MAC or bridging layer.

IPX OPTION BACKGROUND INFORMATION

The Internetwork Packet Exchange (IPX) protocol is a datagram, connectionless protocol in the NetWare environment analogous to the Internet Protocol (IP) in the TCP / IP environment. With the help of Routing Information Protocol (RIP) and Service Advertising Protocol (SAP), the IPX router performs the network layer tasks of addressing, routing and switching information packets, to move packets from one location to another in a complex network.

The CyberSWITCH supports the standard method of routing Novell® IPX datagrams over an internetwork. The system provides bandwidth management features to make the interconnection of IPX networks cost effective over demand type connections like ISDN. Additional security features provide data privacy for Novell networks connected by the system.

Over the last few years Novell has evolved their WAN IPX routing model. Originally the Novell IPX router supported numbered WAN network interfaces only. That is, a unique IPX network number was assigned to each WAN port on the router.

Novell then migrated to an unnumbered WAN network interface in their latest versions of their IPX router. When two routers communicate, they will try to use the unnumbered network interface type. If both routers support this type of interface they will agree on this and initiate data transfer. If one router does not support the unnumbered type, the newer router will defer to the older router and agree to use a numbered type interface. The new router will let the older router assign the network number for the WAN link.

IPX INTERNAL NETWORK NUMBER

CONFIGURING THE IPX INTERNAL NETWORK NUMBER

USING CFGEDIT

1. Press 2 at the IPX menu to configure the IPX internal network number.

2. As prompted, enter the hexadecimal internal network number for the IPX router (the CyberSWITCH). In our example, this is 12F8.

USING MANAGE MODE COMMANDS

ipxinet
Allows you to enter the hexadecimal internal network number for the IPX router.

IPX INTERNAL NETWORK NUMBER CONFIGURATION ELEMENT

IPX INTERNAL NETWORK NUMBER
This number uniquely identifies a specific IPX router in the internetwork. In the Novell environment, an IPX internal network number must be assigned to all IPX file servers, including IPX routers. This number is an arbitrary value, assigned when the IPX router is configured. It may be 1 to 8 hexadecimal digits in length (up to 4 bytes).

IPX NETWORK NUMBER BACKGROUND INFORMATION

Novell NetWare networks use IPX external and internal network numbers. An *IPX internal network number* is a unique identification number assigned to a network server or router at the time of installation. Servers and routers periodically broadcast their numbers across the network to advertise their presence. Each server / router must have a unique internal network number to distinguish itself from other servers / routers. A second address, an *IPX external network number*, must be assigned to identify the network to which the server / router belongs. Unlike the internal network number, all servers / routers connected to the same network must be assigned the same external network number in order to communicate.

IPX NETWORK INTERFACES

The IPX feature on the CyberSWITCH supports the following three network interfaces:

- LAN
- WAN
- Remote LAN

The Remote LAN interface allows the CyberSWITCH to connect to remote bridge devices over the WAN. In other words, when incorporating a Remote LAN interface along with traditional WAN interfaces, the CyberSWITCH can connect to routers or bridges or a mix of both. The CyberSWITCH (acting as an IPX router) treats all bridge devices connected to the Remote LAN as if they were on an Ethernet LAN segment.

Both LAN and Remote LAN network interfaces must be configured. WAN network interfaces, on the other hand, do not explicitly need to be configured. These are dynamically assigned by the CyberSWITCH when a WAN connection is established to another router.

CONFIGURING IPX NETWORK INTERFACES

USING CFGEDIT

1. Press 3 from the IPX menu to configure the IPX interface information.
2. Press 1 to add an interface.
3. Select the interface type from the displayed list (LAN or WAN [Remote LAN]).
4. Enter the user-defined interface name.
5. Enter the hexadecimal IPX external network number for the LAN or the Remote LAN, as applicable.
6. Enter the LAN port number of the interface, if applicable.
7. Select the packet encapsulation type from the displayed list.
8. Enter the MTU size. Note that the maximum value for the MTU size varies based on the packet encapsulation type chosen.

9. If IPX RIP has been enabled for the system, enter the following:
   a. RIP send control (do not respond or respond)
   b. frequency (in seconds) of sending RIP updates
   c. RIP receive control (do not respond or respond)
   d. time (in seconds) to age RIP entries
   e. RIP respond control (do not respond or respond)

10. If IPX SAP has been enabled for the system, enter the following:
   a. SAP send control (do not respond or respond)
   b. frequency (in seconds) of sending SAP updates
   c. SAP receive control (do not respond or respond)
   d. time (in seconds) to age SAP entries
   e. SAP respond control (do not respond or respond)

11. After all the interface information has been entered, a summary screen will be displayed similar to the sample screen below:

```
Current Configuration for INTERFACE "lanport1":

Interface Type            LAN
IPX Network Number        11111111
MTU (bytes)               1497
Encapsulation             Ethernet 802.2
LAN Port                  1
RIP Configuration:
 Send Control             Send
 Send Frequency           60 seconds
 Receive Control          Receive
 RIP entry Ageing Time    180 seconds
 Respond Control          Respond
SAP Configuration:
 Send Control             Send
 Send Frequency           60 seconds
 Receive Control          Receive
 SAP entry Ageing Time    180 seconds
 Respond Control          Respond

Are you sure you want to add the INTERFACE "lanport1" (Y or N) [Y]? Y
```

12. As shown above, enter "Y" to save the interface configuration.

13. Repeat this procedure to add additional interfaces.

USING MANAGE MODE COMMANDS

ipxnetif

Displays the current IPX network interface data.

ipxnetif [add/change/delete]

Allows you to add / change / delete an IPX network interface.

IPX NETWORK INTERFACE CONFIGURATION ELEMENTS

GENERAL IPX NETWORK INTERFACE CONFIGURATION ELEMENTS

INTERFACE TYPE

When configuring an IPX Network interface, this parameter specifies the type of network segment to which the network interface connects. The network Interface type of LAN indicates that the system is physically connected to an Ethernet LAN segment. The WAN (Remote LAN) interface allows the system to connect to remote bridge devices. The traditional WAN interface allows the system to connect to other routers.

In a system using all three interfaces, both the LAN and Remote LAN interfaces must be configured. However, traditional WAN network interfaces do not explicitly need to be configured. These interfaces are dynamically assigned by the system when a WAN connection is established to another IPX router.

IPX NETWORK NUMBERS

Unique, user-assigned numbers (*internal* or *external*) associated with the network. These parameters are hexadecimal values from 1 to 4 bytes in length, and may range from 1 to ffff. (“0” is invalid.) An *IPX internal network number* corresponds to the number assigned to a network server or router. An *IPX external network number* corresponds to a physical network or cable segment (i.e, such as a LAN), which may include multiple servers. Unlike the internal network number, all servers / routers connected to the same network must be assigned the same external network number in order to communicate.

MAXIMUM TRANSMISSION UNIT (MTU)

Specifies the maximum number of bytes that can be transmitted on the network interface. Some devices on the network may not be able to receive large data packets. This parameter allows you to maintain compatibility with these devices by setting the MTU to agree with that supported by the device. This parameter is a decimal value from 60 to 1500, depending on the type of datagram encapsulation selected.

ENCAPSULATION TYPE

Specifies the IPX datagram encapsulation type used by this network interface. NetWare supports 4 types of encapsulation: Novell ETHERNET_SNAP, Novell Ethernet 802.3, Novell ETHERNET_II, Novell Ethernet 802.2. The Ethernet 802.3 type is the default type for NetWare v2.x and v3.x. The Ethernet 802.2 type is the default type for NetWare v4.x. Choose the appropriate encapsulation type for this network segment.

LAN PORT NUMBER

For LAN type network interfaces, this parameter specifies the port number on the Ethernet adapter to which the network interface is physically connected. This parameter is a decimal value from 1 to 2, depending on the system hardware. Note: this parameter is not used for Remote LAN interfaces.

RIP IPX NETWORK INTERFACE CONFIGURATION ELEMENTS

SEND CONTROL

Specifies how the CyberSWITCH will send RIP information on this network interface. If this parameter is set to send, the system will transmit IPX RIP packets on this network interface. If this parameter is set to do not send, the system will not transmit any IPX RIP packets on this network interface.

SEND FREQUENCY
Specifies the frequency at which the system will transmit RIP packets, if the Send control parameter is set to send for this interface. This parameter is a decimal value specified in seconds from 1 to 300. The default value is 60 seconds.

RECEIVE CONTROL
Specifies how the system will process RIP packets received on this network interface. If this parameter is set to receive, the system will process IPX RIP packets received on this network interface and update its internal routing tables. If this parameter is set to do not receive, the system will not process any IPX RIP packets received on this network interface.

RIP ENTRY AGING TIME
Specifies the time it takes for the system to age out and make inactive, a dynamic Routing table entry learned on this network interface. This parameter is a decimal value specified in seconds from 1 to 180. The default is 180 seconds.

RESPOND CONTROL
Specifies how the system should respond to RIP queries from other devices on this network interface. If the parameter is set to respond, the system will transmit a RIP response to the requesting device. If this parameter is set to do not respond, the system will ignore RIP Requests received on this network interface.

SAP IPX NETWORK INTERFACE CONFIGURATION ELEMENTS

SEND CONTROL
Specifies how the system will send SAP information on this network interface. If this parameter is set to send, the system will transmit IPX SAP packets on this network interface. If this parameter is set to do not send, the system will not transmit any IPX SAP packets on this network interface.

SEND FREQUENCY
Specifies the frequency at which the system will transmit SAP update packets, if the Send control parameter is set to send for this interface. This parameter is a decimal value specified in seconds from 1 to 300. The default value is 60 seconds.

RECEIVE CONTROL
Specifies how the system will process SAP packets received on this network interface. If this parameter is set to receive, the system will process IPX SAP packets received on this network interface and update its internal service tables. If this parameter is set to do not receive, the system will not process any IPX SAP packets received on this network interface.

SAP ENTRY AGING TIME
Specifies the time it takes for the system to age out and make inactive, a dynamic Service table entry learned on this network interface. This parameter is a decimal value specified in seconds from 1 to 180. The default is 180 seconds.

RESPOND CONTROL
Specifies how the system should respond to Service queries from other devices on this network interface. If the parameter is set to respond, the system will transmit a SAP response to the requesting device. If this parameter is set to do not respond, the system will ignore Service queries received on this network interface.

IPX NETWORK INTERFACE BACKGROUND INFORMATION

Traditional routing products ask you to define the network interfaces to which the router is directly connected:

LAN INTERFACES

LAN network interfaces are fixed broadcast media type interfaces. These interfaces are assigned a specific network number and all devices on that LAN must agree on the IPX network number used on the LAN segment. The LAN network interface is a regular IPX interface used to connect the system to the LAN. The Ethernet frame types supported under the IPX protocol include:

- Novell 802.3. This is the Novell default frame format for NetWare 2.x and 3.x servers.
- Novell SNAP. The DSAP and SSAP values indicate SNAP encapsulation.
- Ethernet 802.2. The Novell default frame format with NetWare 4.x software for CSMA / CD is Ethernet 802.2. The DSAP and SSAP values indicate that the frame contains an IPX packet.
- Novell Ethernet II. Ethernet protocol id field indicates that the frame contains an IPX packet.

WAN INTERFACES

The CyberSWITCH connects IPX router devices over ISDN and other digital WAN links. Routers operate at the network protocol layer and understand the logical topology of the IPX intranet.

The CyberSWITCH uses the NetWare Routing Information Protocol (RIP) to transmit its routing information on the network. This protocol periodically broadcasts routing table updates on the network. A dynamically learned entry is aged out of the system's routing table if the route entry is not verified by the periodic RIP broadcasts.

In a similar manner, the system uses the NetWare Service Advertisement Protocol (SAP) to transmit its service table information on the network.

The system supports the standard NetWare RIP and SAP protocols as described in the Novell's document, "IPX Routing Specification."

REMOTE LAN INTERFACES

CyberSWITCH uses a Remote LAN interface to connect remote bridge devices to other IPX router network interfaces. The IPX router treats all bridge devices connected to the Remote LAN as if they were on an Ethernet LAN segment. That is, the system emulates an Ethernet medium over the series of ISDN point-to-point connections. The IPX router encapsulates IPX data for the Remote LAN interface in Ethernet packets and forwards the data to the remote bridges.

If the remote LAN only has NetWare clients connected to it, these clients will assume the IPX network number assigned to the Remote LAN interface. For these "simple" remote networks, it is not required to configure an IPX network number for the remote bridge device. When the bridge connects, it looks for the first configured IPX Remote LAN interface, and uses it as a default.

Currently, we do not support a remote LAN with both NetWare servers and clients connected to it.

IPX ROUTING PROTOCOLS

CONFIGURING IPX ROUTING PROTOCOLS

USING CFGEDIT

1. Select *Routing Protocols* from the IPX menu. The following will be displayed:

```
IPX Routing Protocol Menu:

   1)  IPX RIP Processing is currently ENABLED
   2)  IPX RIP Table maximum is 282
   3)  IPX SAP Processing is currently ENABLED
   4)  IPX SAP Table maximum number of entries is 282

Select function from above or <RET> for previous menu:
```

2. To change the enable / disable status for any of the IPX protocols, simply enter the Id number associated with the protocol, and follow the onscreen instructions.

3. To adjust the number of entries in the RIP table, press 2. Enter a value between 20 and 3072.

4. To adjust the number of entries in the SAP table, press 4. Enter a value between 20 and 3072.

USING MANAGE MODE COMMANDS

ipxrip
Displays the current IPX RIP status as either enabled or disabled.

ipxrip [off/on]
Allows you to disable / enable IPX RIP.

ipxsap
Displays the current IPX SAP status as wither enabled or disabled.

ipxsap [off/on]
Allows you to disable / enable IPX SAP.

IPX ROUTING PROTOCOL CONFIGURATION ELEMENTS

IPX RIP PROCESSING OPTION
Specifies whether the system should process the NetWare Routing Information Protocol (RIP). If this option is enabled, you can configure additional RIP options for each network interface, or remote device table entry. If this option is disabled, the system will not process any NetWare RIP packets.

IPX SAP PROCESSING OPTION
Specifies whether the system should process the NetWare Service Advertisement Protocol (SAP). If this option is enabled, you can configure additional SAP options for each network interface, or remote device table entry. If this option is disabled, the system will not process any NetWare SAP packets.

RIP / SAP NUMBER OF TABLE ENTRIES
Specifies the maximum number of routing entries which can be stored in the route or service table. You may select a number between 20 and 3072. The default value is 282 (141 routes + 141 services).

IPX ROUTING PROTOCOL BACKGROUND INFORMATION

Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) are used to automate the exchange of information across a network. These discovery protocols reduce the need to manually update routing and service tables.

IPX RIP is a protocol used to exchange routing information among IPX devices. RIP maintains a routing table of routing information gathered across the network. RIP broadcasts this information (either periodically or *triggered* by events) to update other routers. RIP determines the fastest path between two points on a network in terms of the number of "ticks" between those points.

IPX SAP is a protocol used to exchange service information among IPX devices. Servers use SAP packets to advertise their particular services. Routers retrieve these packets and store them in tables. Like RIP, routers then broadcast this service information to update other routers.

ROUTING/SERVICE TABLES

The system stores IPX routing information in a table. Each time a packet is received, the routing table is referenced to determine to which network interface to forward the packet. There are three types of routes stored in this table:

- static
- RIP (learned)
- internal

Static routes are configured locally on the system. These routes are stored, used internally and advertised to other routers using RIP.

RIP routes are learned from incoming RIP packets. These routes are stored, used internally and advertised to other routers using RIP.

Internal routes are stored and used by the system exclusively. These include routes for:

- the internal network number of this router
- the broadcast address for each IPX network interface configured
- the individual address for each IPX network interface configured

The maximum number of routes to be stored depends on the size and topology of the IPX network. Routers in the same network may have large differences in the maximum number of routes they store just because of their location in the network. Because of these factors, and limited memory in the router, the maximum number of routes for each router must be configurable.

Similarly, the system also stores IPX service information in a table. Each time service information is requested, the service table is referenced to determine the IPX address of the server. The following service entries are stored in this table:

- static
- SAP

Static services are configured locally on the system. *SAP* entries are learned from incoming SAP packets. All services are stored, used internally and advertised to other routers.

The same factors that affect the maximum number of routes stored also affect the maximum number of services stored. Because of these factors, the maximum number of services for each router must be configurable.

Each route or service entry requires memory. So increasing the number of entries may reduce the amount of memory available for other system features (such as compression). Each 1KByte of memory provides approximately 6 route entries or 4 service entries. If you configure the maximum number of table entries allowable (3072), you will consume 471 KB for the routing table, and 639 KB for the service table.

We recommend you size both of these tables to be at least 10% larger than their steady-state size to allow for network growth. However, you may choose a larger or smaller percentage, based on memory availability.

SPECIAL CONSIDERATIONS - REMOTE LAN INTERFACE

If using a router-to-router WAN interface, the routers at both ends participate in RIP and SAP protocols. The routers intelligently process RIP and SAP messages and can be configured to only send them when required. However, if using a Remote LAN interface, one end-point of the connection is a bridge. The bridge does not understand RIP and SAP protocols; therefore, RIP / SAP messages appear as background broadcast traffic. This traffic may cause dial-up links to remain established for long periods of time. For more efficient operation, consider the following when using a remote LAN interface:

- *Link utilization parameters.* Most bridges and routers allow you to configure link utilization thresholds that determine how long a dial-up connection will stay up. If your dial-up link stays up for longer than required, verify that the link utilization parameters are set properly for the connection.
- *Trace facilities.* Many types of background traffic can keep the dial-up connection active. Using a trace facility or traffic analyzer, determine what type of traffic is keeping the link up. If you determine that RIP or SAP traffic is keeping the link up, consider the following:
  a. If the remote LAN has only clients, consider setting the RIP and SAP settings on the interface to *Do Not Send, Receive* and *Respond*. These settings will allow the system to process the clients' requests for servers, yet should prevent the system from keeping the connection up unnecessarily. In addition, consider adding filters to the bridge (to prevent any background traffic from devices on the remote LAN from keeping the line up), or disable the devices' ability to send such traffic in the first place.
  b. If the remote LAN has any servers or routers, the situation becomes more difficult. In such applications, we recommend a router-to-router WAN interface rather than a remote LAN interface. However, if you still want to use a remote LAN interface, consider adjusting throughput monitoring parameters on both peers to drop the connection when only RIP and SAP activity is present. Or, disable RIP and SAP activity altogether and configure static routes and services.
- If phone costs are of no concern, simply enable *Send, Receive,* and *Respond* for both RIP and SAP.

IPX STATIC ROUTES

Note: With the availability of Triggered RIP / SAP (page 343), the configuration of static routes is no longer necessary but still supported. Situations may arise in which a remote router does not support our implementation of Triggered RIP / SAP. In this case, it would be necessary to configure a static route to that particular router.

CONFIGURING IPX STATIC ROUTES

USING CFGEDIT

1. From the *IPX menu*, select *IPX Static Routes*.
2. Select *Add a static route*.
3. Enter the hexadecimal destination IPX network number.
4. Enter the device name or the hexadecimal IPX node address of the next hop device. Note that the remote device name must be present in the on-node device database if the system is configured for device level authentication.
5. Enter the number of hops for this route.
6. Enter the number of ticks for this route.
7. Select a RIP propagation scheme from the displayed list. Note that the third option (propagate only when the Next Hop is connected) is displayed only when the static route Next Hop is accessed over the WAN.
8. After all static route information has been entered, a similar screen will be displayed:

```
There are currently no IPX Static Routes configured.
Enter (1) to Add a STATIC ROUTE or press <RET> for previous menu? 1

Enter the hexadecimal Destination IPX Network Number
   or <RET> to cancel? 33333333

Enter the device name or the hexadecimal IPX Node Address
of the Next Hop device or <RET> to cancel? remote1

Enter the number of hops for this route [default = 2]? 2

Enter the number of ticks for this route [default = 2]? 2

RIP Propagation Control:
   1) Do Not Propagate.
   2) Always Propagate.
   3) Propagate only when the Next Hop is connected.

Enter a RIP Propagation Scheme from the above menu [default = 3]? 3
```

9. Follow the onscreen instructions to save the configured static route information.

USING MANAGE MODE COMMANDS

ipxroute
Displays the current IPX routes (both statically entered and "learned").

ipxroute [add/change/delete]
Allows you to add / change / delete an IPX route.

IPX STATIC ROUTES CONFIGURATION ELEMENTS

DESTINATION NETWORK
The IPX network number reachable through this static route entry. This parameter is a hexadecimal value from 1 to 4 bytes in length.

NEXT HOP
The device name or IPX Network address of the next hop device that provides access to the destination IPX network. If a name is specified, it can be either a on-node device database name or a name configured in an off node authentication server data base. The name must be a valid Device table entry if the system is configured for on-node device table data base authentication. The name is not validated if the system is configured for off-node server authentication. You may specify the IPX Network address of the next hop device for routes accessed via a LAN or a WAN Remote LAN network interface. The IPX network address is specified as a 4 byte hexadecimal IPX network number and a 6 byte hexadecimal node address. The two values are separated by a ":", colon character.

NUMBER OF HOPS
Indicates the number of routers that are traversed in order to reach the destination IPX network. This number is used to calculate the best route to the destination IPX network when multiple routes exists. This parameter is a decimal value from 1 to 15.

NUMBER OF TICKS
Indicates the time, in ticks, that a packet will take to reach the destination IPX network. A tick is approximately 1 / 18th of a second. This number is used to calculate the best route to the destination IPX network when multiple routes exists. This parameter is a decimal value from 1 to 15.

RIP PROPAGATION
Indicates how the system will advertise the IPX route defined by this static route entry. If you choose "Do not Propagate", the system will not advertise this route table entry at any time. If you choose "Always Propagate", the system will advertise this route table entry as part of the normal routing table advertisement protocol processing. If you choose "Propagate only when the Next Hop is connected", the system will only advertise this route table entry if the destination network is reachable over the WAN and the next hop device is actively connected to the system.

IPX STATIC ROUTES BACKGROUND INFORMATION

You may configure static routing entries to access WAN networks that are not directly connected to the system, or to access a LAN network through a router that does not support RIP. IPX static routes specify the IPX network number of the next hop device that provides access to the destination IPX network. The IPX static route is used with the IPX NetWare Static Services configuration to provide a route to servers.

IPX NETWARE STATIC SERVICES

Note: With the availability of Triggered RIP / SAP (page 343), the configuration of static services is no longer necessary but still supported. Situations may arise in which a remote router does not support our implementation of Triggered RIP / SAP. In this case, it would be necessary to configure a static service for that particular router.

CONFIGURING IPX NETWARE STATIC SERVICES

USING CFGEDIT

1. Press 6 from the IPX menu to configure a NetWare static service entry.
2. Press 1 to begin the configuration of a NetWare static service entry.
3. Enter the user-defined service name.
4. Enter the hexadecimal service type.
5. Enter the hexadecimal IPX network number for this service.
6. Enter the hexadecimal IPX node number for this service.
7. Enter the hexadecimal IPX socket number for this service.
8. Enter the number of hops to this service.
9. Select the SAP propagation control. Note that the third option (propagate only when the Next Hop is connected) is displayed only when the static route Next Hop is accessed over the WAN.
10. After all NetWare static service information has been entered, a screen similar to the following sample screen will be displayed:

```
Service Name       Admin
Service Type       0x0004 File Server
Network Address    33333333:0409a0000001:0451
Number of Hops     2
SAP Propagation    Propagate only when the Next Hop is connected

Are you sure you want to add the STATIC Service (Y or N) [Y]? <RET>
```

11. Press "Y" to save the static service configuration.

USING MANAGE MODE COMMANDS

ipxsvc
Displays the current IPX service data (both statically entered and "learned").

ipxsvc [add/change/delete]
Allows you to add / change / delete an IPX service.

IPX NetWare Static Services Configuration Elements

Service Name

Specifies the NetWare service name that is the target of this static service definition. This parameter is a 48 character NetWare service name.

Service Type

Indicates the type of NetWare service that is the target of this static service definition. You may enter the hexadecimal service type value, or request a list of common service types. Some common NetWare service types are

- 0x0004 File Server
- 0x0005 Job Server
- 0x0007 Print Server
- 0x0009 Archive Server
- 0x0047 Advertising Print Server
- 0xFFFF All Services

IPX Network Number

The IPX network number where the service is located. This parameter is a hexadecimal value from 1 to 4 bytes in length.

IPX Node Number

The IPX node number of the NetWare device where the service is located. This parameter is a hexadecimal value 6 bytes in length.

IPX Socket Number

The IPX socket number where the service is located. This parameter is a hexadecimal value 2 bytes in length. Some common IPX Socket numbers are:

- 0x0451 NetWare Core Protocol (File Server)
- 0x0452 Service Advertising protocol
- 0x0453 Routing Information protocol
- 0x0455 NetBIOS Protocol
- 0x0456 Diagnostic packet
- 0x0457 Serialization Packet

Number of Hops

Indicates the number of routers that are traversed in order to reach this Service. This number is used to calculate the best route to the destination Service when multiple routes exists. This parameter is a decimal value from 1 to 15.

SAP Propagation

Indicates how the system will advertise the NetWare Service defined by this static service entry. If you choose "Do not Propagate", the system will not advertise this service table entry at any time. If you choose "Always Propagate", the system will advertise this service table entry as part of the normal service table advertisement protocol processing. If you choose "Propagate only when the Next Hop is connected", the system will only advertise this route table entry if the destination network is reachable over the WAN and the next hop device for the route entry is actively connected to the system.

IPX NETWARE STATIC SERVICES BACKGROUND INFORMATION

This IPX feature allows you to configure service servers that are on networks across the WAN. The IPX NetWare Static Services configuration tells the system which servers are available for access. The static route configuration tells the system how to get to the network on which the servers are located.

IPX SPOOFING

CONFIGURING IPX SPOOFING

USING CFGEDIT

1. Press 7 from the IPX menu to configure IPX spoofing options. The following screen will be displayed. Note that each spoofing parameter has a global flag that controls which spoofing configuration level should be used: system level or device level.

```
IPX Spoofing Menu:

   1) IPX Watchdog Spoofing Configuration
   2) SPX Watchdog Spoofing Configuration
   3) Serialization Packet Handling
   4) Message Packet Handling

Select function from above or <RET> for previous menu:
```

2. Press 1 to configure IPX watchdog spoofing. An IPX watchdog spoofing menu will be displayed.
   a. Press 1 to select the IPX watchdog spoofing configuration level. Follow the onscreen instructions to select either device level or system level spoofing. Return to the IPX watchdog spoofing menu.
      Note: If device level spoofing is selected, the system will use each individual device's spoofing configuration. If system level spoofing is selected, the global spoofing configuration will apply to all devices, regardless of their individual spoofing configurations.
   b. Press 2 to select the system IPX watchdog spoofing level. The default values for all parameters will be displayed. Enter the Id of any parameters you need to change. Follow the onscreen instructions for changing the default values. Return to the IPX spoofing menu.

3. Press 2 to configure SPX watchdog spoofing. An SPX watchdog spoofing menu will be displayed.
   a. Press 1 to select the SPX watchdog spoofing configuration level. Follow the onscreen instructions to select either device level or system level spoofing. Return to the SPX watchdog spoofing menu.
   b. Press 2 to select the system SPX watchdog spoofing level. The default values for all parameters will be displayed. Enter the Id of any parameters you need to change. Follow the onscreen instructions for changing the default values. Return to the IPX spoofing menu.

4. Press 3 to configure the serialization packet handling. A serialization packet handling menu will be displayed.
   a. Press 1 to select the serialization packet handling configuration level. Follow the onscreen instructions to select either device level or system level. Return to the serialization packet handling menu.

b. Press 2 to select the system serialization packet handling level. The default values for all parameters will be displayed. Enter the Id of any parameters you need to change. Follow the onscreen instructions for changing the default values. Return to the IPX spoofing menu.

5. Press 4 to configure the message packet handling. A message packet handling menu will be displayed.
   a. Press 1 to select the message packet handling configuration level. Follow the onscreen instructions to select either device level or system level. Return to the message packet handling menu.
   b. Press 2 to select the system message packet handling level. The default values for all parameters will be displayed. Enter the Id of any parameters you need to change. Follow the onscreen instructions for changing the default values. Return to the IPX spoofing menu.

USING MANAGE MODE COMMANDS

ipxspoof
Allows you to configure system level spoofing data.

IPX SPOOFING CONFIGURATION ELEMENTS

CONFIGURATION LEVEL
Allows you to choose either device level or system level configuration for the following IPX elements:
- IPX watchdog spoofing
- SPX watchdog spoofing
- serial packet handling
- message packet handling

PACKET HANDLING METHOD
Available for Serial Packet Handling and Message Packet Handling. Allows you to select the system level method of handling packets. You may choose from the following packet handling methods:
- always discard
- forward only when connected
- always forward

IPX SPOOFING BACKGROUND INFORMATION

NetWare was designed for the LAN environment, and assumes that there is always available bandwidth. Because of this, NetWare protocols are not well suited to WANs. Special handling must be given to the NetWare protocols to prevent them from causing excessive ISDN connections. The special handling of NetWare protocols in a routing environment consists of spoofing and automatic filters.

Spoofing is a method to prohibit excessive ISDN connections. When a request packet is received that should be routed over the WAN, yet there is no connection up to the remote device, the spoofing process internally generates a desired response packet. The NetWare protocols that require spoofing are the Watchdog Protocol and the Sequence Packet Exchange (SPX) Protocol. Automatic filters are also used to prohibit excessive ISDN connections caused by the NetWare protocols.

WATCHDOG PROTOCOL

Watchdog Protocol is used by NetWare Servers to detect "dead" clients. If no traffic has been seen by a server from an attached client for a configurable amount of time, the server sends a watchdog packet to the client to determine if the client is still alive or merely inactive. If, after a few minutes, a watchdog reply is not received by a server, it is assumed that the client is no longer alive and the connection to the server is terminated.

If no connection exists to a device and the server sends a watchdog request to a remote client, a connection would have to be established to deliver the watchdog request. With watchdog spoofing enabled, a watchdog response is generated internally and delivered to the server as if the packet was sent by the remote client. This satisfies the server without causing a connection to be established. To allow a server to timeout a client that is no longer alive, the watchdog requests are forwarded over the WAN when a connection already exists. In addition, a watchdog spoofing duration time, T, can be specified. When the connection is down to a device and a watchdog request is received that should be forwarded to this device, a watchdog response will be spoofed for T amount of time. After T amount of time, the watchdog request will be filtered without generating a response. The duration timer T starts when a device is disconnected and is reset each time a new connection is established.

This above described implementation will be followed for watchdog request packets received over the LAN and the WAN. If a watchdog request is received over the WAN and it is determined that a spoofed watchdog response should be generated, it will be returned over the same WAN connection on which it was received.

The implementation of watchdog spoofing eliminates unnecessary connections while allowing clients to be aged out and does not require any client side spoofing or end-to-end-protocol.

The parameters for watchdog spoofing are configured for each remote device. The watchdog spoofing option can be enabled or disabled. By default the option is enabled. When disabled the watchdog requests are routed without any special handling. If the option is enabled, the watchdog spoofing duration time T is specified in minutes. The default is set to 120 minutes.

SPX PROTOCOL

SPX Protocol is optionally used by NetWare applications requiring guaranteed, in-sequence delivery of packets by a connection-oriented service. Each end of an SPX connection sends keep-alive packets, identified as <SYS> packets, to monitor the status of the connection.

The SPX protocol ensures connection integrity by exchanging a keep-alive packet between the connection end-points, once every 6 seconds. If an SPX keep-alive packet is received that is destined for a remote device and no connection exists to the device, a connection would have to be established to deliver the packet. The keep-alive packets are handled using the same approach being used for server watchdog request packets. With SPX spoofing enabled, a keep-alive is generated internally and delivered to the local endpoint as if the packet was sent by the remote endpoint. This satisfies the local endpoint without causing a connection to be established. To allow an SPX connection to timeout the keep-alives are forwarded over the WAN when a connection already exists. In addition, an SPX spoofing duration time T can be specified. When the connection is down to a device and a keep-alive is received that should be forwarded to this device, a keep-alive will be spoofed for T amount of time. After T amount of time, the keep-alive will be filtered without generating a keep-alive response. The duration timer T starts when a device is disconnected and is reset each time a new connection is established.

Some of these <SYS> packets are overloaded in that they are not just keep-alive packets but are control packets needed for the application to run successfully and hence have to be routed like regular SPX data packets. If any NetWare application does not seem to work across WANs, it may be because of the mishandling of these <SYS> packets and can be traced by disabling SPX keep-alive spoofing.

This above described implementation is followed for keep-alive packets received over the LAN and the WAN. If a keep-alive is received over the WAN and it is determined that a spoofed keep-alive should be generated, it will be returned over the same WAN connection on which it was received.

The parameters for SPX spoofing are configured for each device. The SPX spoofing option can be enabled or disabled. By default the option is enabled. When disabled the SPX keep alives are routed without any special handling. If the option is enabled the SPX spoofing duration time T is specified in minutes. The default is set to 120 minutes.

IPX TYPE 20 PACKET HANDLING

CONFIGURING IPX TYPE 20 PACKET HANDLING

USING CFGEDIT

1. Press 8 from the IPX menu to configure IPX type 20 packet handling. The following screen will be displayed:

```
IPX Type 20 Packet Handling Menu:

   1) IPX Type 20 Packets WAN Forwarding (Enable/Disable)
   2) IPX Type 20 Forwarding Devices.

Select function from above or <RET> for previous menu:
```

2. Press 1 to enable IPX type 20 packet WAN forwarding. Follow the onscreen instructions to complete the enable process. Return to the IPX type 20 handling menu.

3. Press 2 to add IPX type 20 packet WAN forwarding devices.
   a. Press 1 to add a device.
   b. Enter the device's name.
   c. From the displayed list, select an IPX type 20 packet forward control method.

USING MANAGE MODE COMMANDS

ipxt20
Allows you to configure IPX type 20 information.

IPX TYPE 20 PACKET HANDLING CONFIGURATION ELEMENTS

IPX TYPE 20 PACKET HANDLING STATUS
You may enable or disable IPX type 20 packet WAN forwarding. When it is enabled, you may specify devices that can use this feature.

IPX TYPE 20 PACKET HANDLING DEVICE CONFIGURATION ELEMENTS

Once you enable the feature, you can then enter devices to use the feature. The following configuration elements are entered for each device.

IPX TYPE 20 PACKET DEVICES
The device name of the previously configured device.

IPX TYPE 20 PACKET FORWARD CONTROL METHOD
Allows you to determine under what conditions IPX type 20 broadcast packets will be broadcasted to the designated device.

IPX TYPE 20 PACKET HANDLING BACKGROUND INFORMATION

In order for certain protocol implementations, such as NetBIOS, to function in the NetWare environment, routes must allow a broadcast packet to be propagated throughout an IPX internet. The IPX type 20 packet is used specifically for this purpose.

However, it is not practical, nor sometimes desirable, to propagate broadcast packets over the WAN. To help you control IPX type 20 packets more flexibly, this configuration allows IPX type 20 broadcast packets to be propagated to only certain remote devices under certain conditions (for example, only when the connection is up, or always).

IPX ISOLATED MODE

CONFIGURING IPX ISOLATED MODE

USING CFGEDIT

1. Press 9 from the IPX menu to configure the IPX isolated mode.
2. Follow the onscreen instructions to enable or disable the IPX isolated mode.

USING MANAGE MODE COMMANDS

ipxiso
Allows you to enable / disable IPX isolated mode.

IPX ISOLATED MODE CONFIGURATION ELEMENTS

Isolated Mode Status
You may enable or disable the isolated mode.

IPX ISOLATED MODE BACKGROUND INFORMATION

When operating with isolated mode enabled, the CyberSWITCH does not relay IPX datagrams received from the WAN to other IPX routers / hosts located on the WAN. IPX datagrams received from the WAN will be discarded if they need to be forwarded over the WAN. IPX datagrams received on the LAN interface are forwarded to the proper interface.

IPX TRIGGERED RIP/SAP

IPX Triggered RIP/SAP is a type of broadcast protocol used over WAN circuits for router-to-router exchange of route and service information. Its broadcasts are "triggered" by events such as updates or changes to route and service tables. Triggered RIP / SAP offers an alternative to running periodic broadcasts over the WAN, and is especially useful when you consider the costs of periodic broadcasts over WAN links.

Triggered RIP and triggered SAP are user-configurable items which you enable in the on-node device database (page 345). Under the *Options* Menu, *IPX Routing*, *Triggered RIP/SAP*, you can display the devices already configured for these features (i.e., the WAN peer list), as well as configure global timers (applicable to the RIP or SAP update packets).

DISPLAYING WAN PEER LIST

1. Select *Triggered RIP/SAP* from IPX Routing Menu. A menu similar to the following will be displayed:

```
IPX Triggered RIP/SAP Configuration

1)  WAN Peer List
2)  Global Triggered RIP/SAP Timers

Select function from above or <RET> for previous menu:
```

2. Select *WAN Peer List*. The system displays the configured devices for which the triggered RIP / SAP feature enabled. It also displays the WAN peer type as active or passive (page 348).

Keep in mind that you cannot make changes from this menu; you can only display information. To make changes to the WAN peer list, go to the Device Table Menu (page 344).

CONFIGURING TRIGGERED RIP/SAP GLOBAL TIMERS

USING CFGEDIT

1. Select *Triggered RIP/SAP* from the IPX Routing Menu.
2. Select *Global Triggered RIP/SAP Timers*. A menu similar to the following will be displayed:

```
Global Triggered RIP/SAP Timers Options:

                                          Current Settings

1)     Database Timer                   180 sec.
2)     Hold Down Timer1                  20 sec.
3)     Retransmission Timer               5 sec.
4)     Poll Timer                         5 min.
5)     Over Subscription Timer          180 sec.
6)     Maximum Retransmissions           10

Select function or press <RET> for previous menu:
```

3. Select the option you want to adjust.
4. Enter the new value.

CONFIGURATION ELEMENTS

DATABASE TIMER

This timer starts when an update response is received. While this timer is running, the routes learned from this router are still considered *reachable*, and advertised as such on other interfaces. When this timer expires, the routes are considered *unreachable* and advertised as such until the hold-down timer expires. Valid range for timer: 1 to 10,000 seconds; default: 180 seconds.

HOLD-DOWN TIMER

While this timer is running, *unreachable* routes are advertised on other interfaces. This timer starts when:

- the database timer for the route expires
- a formerly reachable route changes to unreachable in an incoming response
- a WAN circuit goes down

When this timer expires, and the unreachability information is communicated to all the reachable WAN routers, this route is deleted. Valid range for timer: 1 to 10,000 seconds; default: 120 seconds.

RETRANSMISSION TIMER

This timer starts when an update request (or response) packet is sent out. If acknowledgment is not received by the time this timer expires, the packet is retransmitted. Valid range for timer: 1 to 10,000 seconds; default: 5 seconds.

MAXIMUM RETRANSMISSIONS

This provides a limit on the number of retransmission attempts for an update request (or response) packet. Maximum number supported: 10.

POLLING TIMER

This is the frequency (in minutes) in which the next-hop WAN router is polled with update requests, once the maximum retransmission count threshold is exceeded. Polling takes place only when there is a physical connection; polling does not initiate its own connection. Valid range for timer: 1 to 10,000 seconds (165 minutes); default: 5 minutes.

OVER-SUBSCRIPTION TIMER

Over subscription is the situation in which there are more next-hop routers on the WAN that need updates than there are channels available. When a WAN circuit goes down, a delay (per the over-subscription timer) is incorporated in marking the routes unreachable. This allows the calls to time-multiplex over the limited channels. Valid range for timer: 1 to 10,000 seconds; default: 180 seconds.

TRIGGERED RIP/SAP BACKGROUND INFORMATION

When there are a large number of remote destinations, the manual configuration of static routes and services over WAN circuits can pose a burden on system management. Yet running RIP / SAP could also be problematic; since these are broadcast protocols, periodic broadcasts may not be feasible due to cost and bandwidth considerations. Enabling the Triggered RIP / SAP feature allows the CyberSWITCH to send information on the WAN only when there has been an *update to the database* or a *change in the reachability* of a next-hop router.

Specifically, triggered RIP and SAP updates are only transmitted on the WAN:

- when a specific request for a routing / service update has been received;
- when the routing or service databases are modified by new information from another interface (in which case, only the latest changes are sent);
- when a destination has changed from an unreachable to a reachable state; and
- when the unit is powered up.

You may customize triggered RIP / SAP operation to your system's specific needs through the global timers. The global timers are user-controlled; they are described in detail in the *Configuration Elements* section (page 343), and include the following:

- database timer
- hold-down timer
- retransmission timer
- polling timer
- over-subscription timer

IPX-SPECIFIC INFORMATION FOR DEVICES

Note: The *Configuring Device Level Databases* chapter contains general information needed to configure on-node device entries. The following sections provide instructions for entering on-node device information specific to IPX routing and / or bridging using the IPX Remote LAN interface.

CONFIGURING IPX DEVICES

WAN DEVICES

USING CFGEDIT

1. Select *Security* from the main menu.
2. Select *Device Level Databases* from the security menu.
3. Select *On-node Device Entries* from the authentication database menu.
4. Press 1 to add a device.
5. Enter the device's name and press <RET>. You should provide *ISDN* (or alternate access information) and *Authentication* information first.
6. Select *IPX*. A screen similar to the following will be displayed:

```
Device IPX Configuration Menu: (Device = "remote1")

1)  IPX Routing               DISABLED
2)  Make calls for IPX data   DISABLED
3)  IPXWAN Protocol           DISABLED
4)  Routing Protocol          NONE
5)  IPX External WAN Net Num  NONE
6)  Spoofing Options

Select function from above or <RET> for previous menu:
```

7. Enable IPX routing. Select *IPX Routing* and follow on-screen instructions.

8. Enable make calls feature. Select *Make calls for IPX data* and follow on-screen instructions only if the CyberSWITCH is to dial-out to remote1.

9. Although *IPXWAN Protocol* appears on the menu, the feature is not yet completely functional.

10. Select *Routing Protocol*. A menu similar to the following will be displayed:

```
IPX Device Routing Protocol Menu:

1)  None
2)  RIP/SAP
3)  Triggered RIP/SAP

Enter selection or press <RET> for previous menu [default=None}:3

1)  ACTIVE
2)  PASSIVE

Triggered RIP/SAP WAN Peer type [default=ACTIVE]: 1
```

11. Select routing protocol. When you select *Triggered RIP/SAP*, you will need to identify the WAN peer type as either *active* or *passive*. An active peer receives broadcasts at all times; a passive peer receives broadcasts only when a connection is up.

12. If you plan to use IPX over Frame Relay, and if you are also using a CSX200 or CSX400 on the other side of the Frame Relay connection, select *IPX External WAN Net Num*. Provide a unique number that you will also reflect on the CSX200 or CSX400 platform.

13. Select *Spoofing Options*. Make changes to default spoofing setup, if desired, through the following menu:

```
IPX Device Spoofing Menu:

   1)  IPX Watchdog Spoofing
   2)  SPX Watchdog Spoofing
   3)  Serialization Packet Handling
   4)  Message Packet Handling

Select function from above or <RET> for previous menu: 1
```

    a. Press 1 to configure IPX watchdog spoofing. The following menu will be displayed:

```
Device Level IPX Watchdog Spoofing Menu:

 1) Default Handling                                  is Discard
 2) Handling while the connection is up               is Forward
 3) Handling for the special period after disconnecting is Spoof
 4) Special period of time after disconnecting       is 120 Minutes

Select function from above or <RET> for previous menu:
```

    b. The screen includes default configuration values. If needed, make changes to the default values.

c. Press <RET> to return to the IPX Device Spoofing menu. Press 2 to configure SPX Watchdog Spoofing. The following menu will be displayed:

```
Device Level SPX Watchdog Spoofing Menu:

 1) Default Handling                                    is Discard
 2) Handling while the connection is up                 is Forward
 3) Handling for the special period after disconnecting is Spoof
 4) Special period of time after disconnecting         is 120 Minutes

Select function from above or <RET> for previous menu:
```

d. The screen includes default configuration values. If needed, make changes to the default values.

e. Press <RET> to return to the IPX Device Spoofing menu. Press 3 to configure serialization packet handling. The following menu will be displayed:

```
Serialization Packet Handling:
   1)  Always Discard
   2)  Forward only when the connection is up
   3)  Always Forward

Current Serialization Packet Handling is "Forward only when the connection is up".

Select function from above or <RET> for previous menu: 1
```

f. The screen includes default configuration values. If needed, make changes to the default values.

g. Press <RET> to return to the IPX Device Spoofing menu. Press 4 to configure message packet handling. The following menu will be displayed:

```
Message Packet Handling:
   1)  Always Discard
   2)  Forward only when the connection is up
   3)  Always Forward

Current Message Packet Handling is "Forward only when the connection is up".

Select function from above or <RET> for previous menu: <RET>
```

h. The screen includes default configuration values. If needed, make changes to the default values.

REMOTE LAN DEVICES

Remote LAN devices are configured in a slightly different way than WAN devices. Since the remote device is a bridge and not an IPX router, the IPX options for Remote LAN devices are configured under the bridge-level options, as follows:

USING CFGEDIT

1. Select *Security* from the main menu.

2. Select *Device Level Databases* from the security menu.

3. Select *On-node Device Entries* from the device level databases menu.

4. Press 1 to add a device.

5. Enter the device's name and press <RET>. You should provide *ISDN* and *Authentication* information first.

6. Select *Bridging* from the Device Table Menu. A menu similar to the following will be displayed:

```
Device Bridging: (Device = "remote2")

   1)  IP (Sub)Network Number        NONE
   2)  Bridging                      ENABLED
   3)  Make calls for bridge data    DISABLED
   4)  IPX Remote LAN Network Number NONE
   5)  IPX Spoofing Options
   6)  AppleTalk Network Number      NONE

Select function from above or <RET> for previous menu?
```

7. Enable *Bridging* and disable *Make calls for bridge data*.

8. Select *IPX Remote LAN Network Number*. Provide the external network number for the Remote LAN interface if desired. The default value, *NONE*, means the remote IPX external number will be the default IPX Remote LAN interface network number. Refer to page 329.

Note: The IPX Spoofing Options selection for Remote LAN devices is for a future release. Do not try to configure at this time.

USING MANAGE MODE COMMANDS

device add

Allows you to add a device entry to the Device List. You will be prompted for device information, including IPX information.

device change

Allows you to change information for a specific device entry. This will allow you, for example, to add IPX information to a previously configured device entry.

IPX CONFIGURATION ELEMENTS FOR DEVICES

IPX ROUTING

Indicates that the remote device is an IPX router and that the system should route IPX datagrams to this device. The system will forward IPX datagrams to this device based on IPX network layer information if this parameter is set to enabled. The system will not forward IPX datagrams to this device based on IPX network layer information if this parameter is set to disabled.

MAKE CALLS FOR IPX DATA

Indicates whether the CyberSWITCH should establish a WAN connection in order to forward IPX datagrams to this remote device. If the CyberSWITCH is properly configured for dial out, and if the remote device has IPX routing enabled and this *Make Calls* option enabled, then the CyberSWITCH will establish a WAN connection to this remote device in order to forward IPX datagrams.

Otherwise, a WAN connection is not established. With triggered RIP/SAP, this field must also be enabled for an active *WAN peer type* to function properly.

IPXWAN PROTOCOL
The IPXWAN protocol option is not yet completely functional. In the future, it will provide interoperability with Novell products.

IPX ROUTING PROTOCOL
Indicates the method, if any, the remote device will be using to maintain routes and service tables.

NONE
Specifies no RIP and SAP protocols (neither periodic nor triggered). You must configure static routes and static services.

Use the *NONE* option when the remote device, such as a single client, does not support standard RIP/SAP or triggered RIP/SAP.

RIP/SAP
Specifies NetWare Routing Information Protocol (RIP) or NetWare Service Advertisement Protocol (SAP). IPX RIP/SAP are broadcast protocols; if enabled, RIP/SAP periodically broadcast routing/service information across WAN circuits. If enabled, you can configure additional RIP/SAP options for this entry. If disabled, the CyberSWITCH will not process any NetWare RIP/SAP packets.

TRIGGERED RIP/SAP
Specifies a modified version of RIP/SAP in which information is broadcast on the WAN only when there has been an update to the RIP or SAP tables or a change in the reachability of a next hop router.

WAN PEER TYPE
WAN peer type applies to triggered RIP/SAP only. The peer type determines how broadcasts are handled for a specific device if something in the RIP/SAP table changes:

ACTIVE
An *active* WAN peer receives broadcasts and conveyed information at all times.

PASSIVE
A *passive* WAN peer receives broadcasts and/or conveyed information only when a connection is up between the router and the WAN peer.

Note that you must enable the *Make Calls* field and define the WAN peer type as *active* before the CyberSWITCH will dial out to this remote device with triggered RIP/SAP updates.

BRIDGING
Defines the remote device as a bridge and not an IPX router. Since bridges operate at the MAC layer, the system must provide MAC layer emulation for remote bridge devices, while continuing to route the network layer IPX protocol. This field must be enabled for remote LAN devices.

MAKE CALLS FOR BRIDGE DATA
This feature is not yet supported for IPX Remote LANs. Therefore, leave this element disabled.

IPX EXTERNAL WAN NETWORK NUMBER
Specifies a user-configurable IPX external network number on the WAN. This parameter can be a hexadecimal value from 1 to 4 bytes in length.The default value is *none*.

This parameter is only necessary for IPX over Frame Relay when at least one of the CyberSWITCHes in the Frame Relay connection is a CSX200 or CSX400. (CSX200 and CSX400 platforms do not support unnumbered connections). In this instance, you must specify the same number on both CyberSWITCHes supporting the Frame Relay access.

IPX REMOTE LAN NETWORK NUMBER
Specifies the IPX external network number on the remote LAN. The default value is *none*.

If you choose to change this parameter, you must specify the IPX external network number used on the remote LAN in question. This value must be the same as the value configured for the corresponding IPX Remote LAN interface.

If this parameter remains *none*, the CyberSWITCH will assume the network number is that of the first configured IPX Remote LAN interface. This is convenient in applications in which remote LANs consist only of clients (thus no explicit external network address), all of which are on the same external virtual LAN.

IPX SPOOFING OPTIONS
For IPX routing, IPX spoofing options are configurable by device, and correspond to the system-level spoofing options.

For IPX Remote LAN devices, IPX spoofing options are currently not available.

IPX BACKGROUND INFORMATION FOR DEVICES

To configure your CyberSWITCH for IPX routing, you must properly complete the system parameters that are IPX-specific. These parameters are discussed in the first portion of this chapter. But, for a remote device to be able to participate in IPX routing or bridging using the IPX Remote LAN interface, you also need to configure that device with the necessary IPX information. This information is configured in the on-node device database.

IPX TRIGGERED RIP/SAP DEVICE BACKGROUND

On the on-node device database, choose Triggered RIP/SAP as the IPX protocol for those remote devices that will use this protocol to exchange route/service information with the CyberSWITCH. You can display these locally-configured remote devices from the WAN peer list.

When using an off-node server, you need to configure a list of IPX Triggered RIP/SAP routers.

At initialization time, Triggered RIP/SAP starts for all on-node devices whose selected protocol is Triggered RIP/SAP. The information about IPX Triggered RIP/SAP may be fetched from an off-node server, if applicable, and then Triggered RIP/SAP will start for the configured routers.

CONFIGURING SNMP

OVERVIEW

A Network Management Station (NMS) is a device that contains SNMP-specific software, giving it the ability to query SNMPAgents using various SNMP commands. If you have purchased an NMS (such as Cabletron's SPECTRUM® Management Platform), you should enable and configure the CyberSWITCH to be an SNMP Agent. This will allow you to use the NMS to monitor the CyberSWITCH and other remote devices on your network. (Refer to *Remote Management: SNMP*.)

On the CyberSWITCH, SNMP is disabled when you first install your system software. (This is the default.) To enable the CyberSWITCH as an SNMP agent, you must first enable IP routing, then configure SNMP. SNMP configuration steps include:

- enabling IP routing (if not already enabled)
- enabling SNMP
- entering Community Name information
- entering SNMP trap information (optional)
- changing the MIB-2 system group objects (optional)

Notes: The SNMP management station must have the latest enterprise MIB (the `ih_mib.asn` file), and the CyberSWITCH must be running the latest software release to take advantage of the available SNMP features.

If you are using Cabletron's SPECTRUM® Element Manager™ as NMS, the enterprise MIB is already built into its software.

If you are using a non-Cabletron product for NMS, you must perform a copy and compile of the latest enterprise MIB (i.e., the `ih_mib.asn` file) on the NMS before beginning the CyberSWITCH SNMP configuration.

If the NMS SNMP software requires the MIB objects that it manages to be defined in a format other than ASN.1, the NMS must have some type of "MIB Formatter" or "MIB Compiler" software. A MIB formatter is SNMP Management Station vendor-specific software that converts MIB data from ASN.1 format to the format understood by the given manager. This MIB Formatter software should be executed using the `ih_mib.asn` file as input.

CONFIGURING SNMP

USING CFGEDIT

Before configuring the SNMP Agent, you must have the following information:

- the Community Name(s) used in SNMP request messages generated by the Network Management Station
- the IP address of the Network Management Station
- the Community Name to be used in Trap messages received by the Network Management Station

The steps to configure SNMP are:

1. Enable IP routing if you have not already done so.

2. Select *SNMP* from the Options menu.

3. Follow the onscreen instructions to enable SNMP. The following SNMP menu will then be displayed:

```
SNMP Menu:

   1)  SNMP (Enable/Disable)
   2)  SNMP Community Name
   3)  SNMP Trap Information
   4)  MIB-2 System Group Objects

Select function from above or <RET> for previous menu:
```

4. Enter the Community Name information.
   a. Enter a user-defined Community Name. This is a case-sensitive string of octets used to identify the community to which an SNMP Manager, along with the Agent(s) that it manages, belongs. It is used to authenticate an SNMP PDU. The string “public” is a widely used Community Name.
   b. Select the access level associated with the Community Name.

5. Enter the SNMP trap information (optional).
   a. Configure IP address(es) and Community Name used in SNMP Trap PDUs.
      - Enter the IP address of the NMS(s) that should receive the traps. The NMS is a device that contains SNMP management software. A Network Manager can be any type of computer that is capable of executing the necessary SNMP management software.
      - Select the Community Name.
   b. If you want authentication failure traps, follow the onscreen instructions for enabling them.
   c. If you want ISDN B-channel usage traps, follow the onscreen instructions for enabling them.
   d. Set the threshold value for ISDN B-channel usage traps.

6. Optional: change the values of the MIB-2 system group objects.

USING MANAGE MODE COMMANDS

Currently you cannot configure SNMP using the Manage Mode, but the following command is available:

snmp

This Manage Mode command displays the current SNMP configuration data. An example output screen is shown below:

```
MANAGE> SNMP

The SNMP feature is enabled.

Current SNMP COMMUNITY NAME Configuration:

id     MIB ACCESS LEVEL       COMMUNITY NAME
---    ----------------------------------------
1      MIB_ADMIN                public
2      MIB_USER                 user
3      MIB_ADMIN                test

Current SNMP TRAP RECEIVER List Configuration:

id     IP ADDRESS               COMMUNITY NAME
-------------------------------------------
1      128.111.001.001          public
2      144.123.111.099          public
3      102.003.003.222          test

The generation of Authentication Failure Traps is disabled.

The generation of ISDN B-Channel Usage Traps is enabled.
The ISDN B-Channel Usage Trap threshold is 5 B-Channels.
```

SNMP CONFIGURATION ELEMENTS

SNMP STATUS

You may enable or disable the SNMP feature.

COMMUNITY NAME

A 1 to 20 character case-sensitive string that specifies a Community Name that will be accepted by the SNMP Agent if it is specified in an incoming Request PDU.

MIB ACCESS LEVEL

The MIB Access Level associated with a Community Name must be selected from the supplied list. It dictates the level of access available to the associated Community Name. The following is a chart of the three possible access levels and their access privileges.

Access Level	*Access Privileges*
MIB GUEST	get (read) MIB-2 system group only
MIB USER	get (read) all MIB-2 and Enterprise MIB objects
MIB ADMIN	get (read) all MIB objects and set (write) all MIB objects that are writable

IP ADDRESS
The IP address assigned to the management station that should receive Trap PDUs.

COMMUNITY NAME
A list of configured Community Names will be displayed. Select the Community Name that should be inserted in the Trap PDUs to be sent to the NMS with the corresponding IP address.

AUTHENTICATION FAILURE TRAPS STATUS
You may enable or disable the generation of SNMP Authentication Failure Traps. The snmpEnableAuthenTraps object of the MIB-2 SNMP group will be initialized to the enabled status that is configured here.

ISDN B-CHANNEL USAGE TRAPS STATUS
You may enable or disable the generation of ISDN B-Channel Usage Traps. You can use these generated traps to monitor the system's ISDN B-channel usage. There are two distinct ISDN B-Channel Usage Traps. The isdnUsageHigh trap is generated when the configured B-channel threshold (refer to the threshold parameter described below) is met or exceeded. The isdnUsageNormal trap is generated when the number of B-channels in use drops back below the configured threshold value.

In addition, the `isdn usage` console command will display B-channel information to aid in monitoring the B-channel usage. Refer to the *System Commands* chapter's *ISDN Usage Related Commands* section for information regarding this command. The generated B-Channel Usage Traps and information displayed by the `isdn usage` console command can help you to determine if additional lines and / or systems are necessary.

ISDN B-CHANNEL USAGE TRAP THRESHOLD
This configured value is used to trigger the ISDN B-Channel Usage Traps. The threshold value is a number between 1 and the total number of available B-channels.

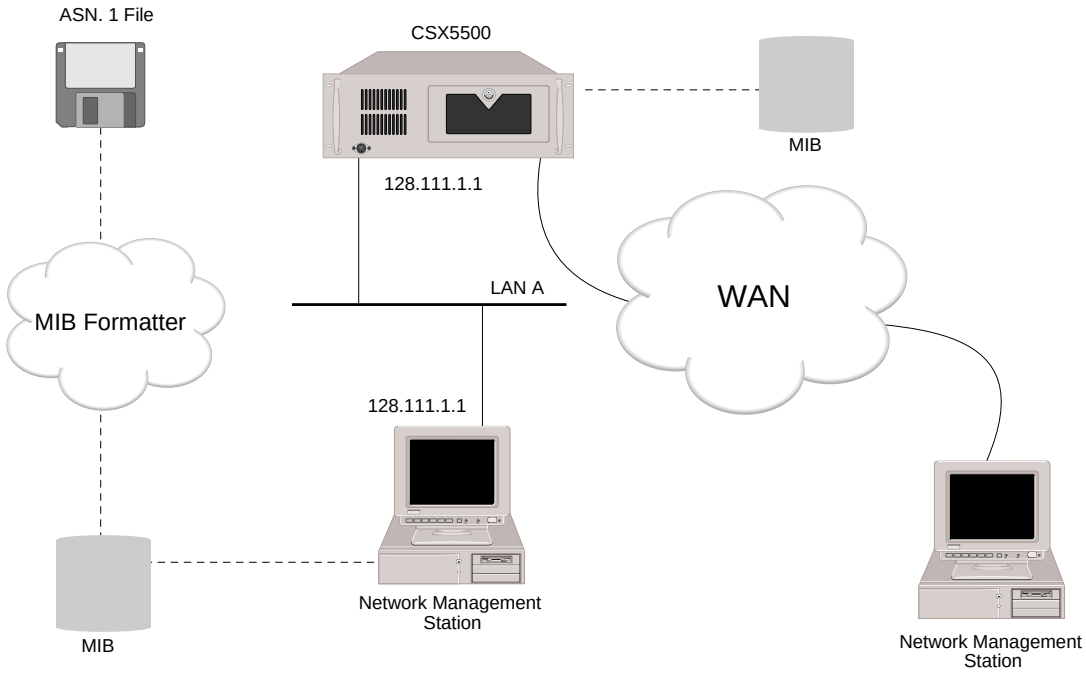
SYSCONTACT
The textual identification of the contact person for this managed node, together with information on how to contact this person. sysContact is a string of 1 to 80 characters.

SYSNAME
The assigned name for this managed node. sysName is a string of 1 to 80 characters.

SYSLOCATION
The physical location of this node (for example: telephone closet, third floor). sysLocation is a string of 1 to 80 characters.

SNMP BACKGROUND INFORMATION

The SNMP Agent allows the system to be monitored from a local and / or a remote Network Management Station (NMS) via the Simple Network Management Protocol. The User Datagram Protocol (UDP) and the Internet Protocol (IP) are used by the SNMP Agent to provide the transport datagram service needed to exchange SNMP messages. Thus only those systems that have enabled the IP routing operating mode can make use of SNMP.



The SNMP Agent will process all SNMP Protocol Data Units (PDUs) which are received at a LAN port or which are received at a WAN port. (A PDU contains both data and control (protocol) information that allows the two processes to coordinate their interactions. The SNMP feature has five types of PDUs: GetRequests, GetNextRequests, GetResponses, SetRequests, and Traps.) This is shown in the above illustration, which depicts a network in which the Network Management Station on LAN A or the remote NMS can manage the system.

All SNMP GetRequest, GetNextRequest, and SetRequest PDUs will be parsed and processed by the SNMP Agent, and an appropriate GetResponse PDU will be generated in response to each valid request PDU. In addition, to ensure security, each incoming PDU will be authenticated by the SNMP Agent. The authentication scheme makes use of a table of Community Name / MIB-access-level pairs, which is searched to determine if the Community Name specified in an incoming request PDU is valid. If the Community Name is valid, the corresponding MIB access level is then checked to determine if the Community Name has the access rights needed to perform the desired PDU action. If either the Community Name or the MIB access right level is invalid, the SNMP Agent will discard the request PDU.

The collection of data objects that can be managed using the GetRequest, GetNextRequest, and SetRequest PDUs is known as the Management Information Base (MIB). The MIB maintained by the SNMP Agent consists of a universal standard set of objects, known as MIB-2, as well as a set of objects that are specific to the system, known as the Enterprise MIB.

The definition for MIB-2 is given in RFC (Request For Comments) 1213: "Management Information Base for Network Management of TCP / IP-based Internets: MIB-II."

The SNMP Agent supports the following MIB-2 groups: the System group, the Interfaces group, the Address Translation (AT) group, the Internet Protocol (IP) group, the Internet Control Message

Protocol (ICMP) group, the User Datagram Protocol (UDP) group, the Transmission Control Protocol (TCP) group, and the Simple Network Management Protocol (SNMP) group.

Currently, each object in the above MIB-2 groups can be retrieved via an SNMP GetRequest or GetNextRequest PDU. However, only the snmpEnableAuthenTraps object in the SNMP group can be changed via the SNMP SetRequest PDU.

Note: Any system object that is changed via an SNMP SetRequest will be returned to its initial value when that system is restarted due to power loss or the action of an system operator.

The definition for the Enterprise portion of the MIB is given in the `ih_mib.asn` file on the system software. The Enterprise MIB consists of four main groups: the ih000ConfigData group, which contains the configuration data for the system; the ih000Statistics group, which contains run-time statistics which are maintained by the system; the ih000StatusReports group, which can be used to remotely display the report status log messages that appear at the administrative console when the *dr* command is entered; and the ihSystemMonitor group, which can be used to monitor system status information such as the status of the system's interfaces, the usage of ISDN B-channels, and information regarding connected devices. Refer to the ASN.1 format of the Enterprise MIB in the `ih_mib.asn` file on the system software for more information on the Enterprise MIB.

In addition to the use of SNMP Request and Response PDUs to exchange data, the SNMP Agent will also generate SNMP Trap PDUs to inform the Network Management Station of important system events. Whenever such an event occurs, the appropriate SNMP Trap PDU will be sent to each NMS that has been configured as a Trap Receiver using the CFGEDIT utility. The NMS that receives the Trap can be attached to the same LAN as the sending system, or it can be attached to a remote LAN.

The current set of Traps that the SNMP Agent will generate include generic traps and enterprise traps. The following generic traps are available:

- coldStart Trap
  An Agent will generate a coldStart Trap PDU at startup time.

- linkUp Trap
  An SNMP Agent will generate a linkUp Trap PDU when the Agent detects that a new link has been placed in service.

- linkDown Trap
  An SNMP Agent will generate a linkDown Trap PDU when the Agent detects that a link has been removed from service.

- authenticationFailure Trap
  An SNMP Agent will generate an authenticationFailure Trap PDU when a PDU with an unknown Community Name or an invalid MIB access level has been received.

The following enterprise traps are available:

- isdnUsageHigh Trap
  An SNMP Agent will generate an isdnUsageHigh Trap PDU when the Agent detects that the number of B-Channels in use meets or exceeds the configured B-Channel threshold. The enabling of this trap and its threshold value are configured through the CFGEDIT configuration utility.

- isdnUsageNormal Trap
  An SNMP Agent will generate an isdnUsageNormal Trap PDU when the Agent detects that the number of B-Channels in use has returned to a value below the configured threshold value.

- authTimeout Trap
  An SNMP Agent will generate an authTimeout Trap PDU anytime an off-node server times out.

- clidDisconnect Trap
  An SNMP Agent will generate an clidDisconnect Trap PDU anytime there is a configuration problem with a device's Calling Line Id.

- cdrOutOfBuffer
  The number of times a buffer was unavailable to send a CDR report record. In this case, the intended record is discarded.

USING CABLETRON NMS SYSTEMS

Cabletron's Enterprise MIB object support within the UAA environment provides a mechanism for Cabletron's SPECTRUM® family of NMS applications to recognize CyberSWITCH products and summon specific information. The additional Enterprise MIBs now supported on the CyberSWITCH are:

- CT-CONTAINER-MIB
- CT-WAN-MIB
- CTMIB2-EXT-MIB

Each of these MIB entries are central to the CyberSWITCH. They provide information on:

- how a device is physically and logically configured
- LAN/WAN connection capability, and
- network interface structure

All objects in these MIBs are implemented as ANS.1/BER *read-only* access types.

CONFIGURING APPLETALK ROUTING

OVERVIEW

The AppleTalk routing feature allows the CyberSWITCH to efficiently route AppleTalk data as opposed to bridging all data relating to the protocol. With the addition of the AppleTalk Remote LAN feature, the CyberSWITCH can be configured to be a router, bridge or a mix of both when handling AppleTalk traffic.

By default, AppleTalk routing is disabled when you first install your system software. To configure the AppleTalk routing feature:

- enable AppleTalk routing
- configure AppleTalk port information
- configure AppleTalk static routes (optional)
- configure AppleTalk capacities
- enable / disable the AppleTalk isolated mode (optional)

APPLETALK ROUTING OPTION

ENABLING APPLETALK ROUTING

USING CFGEDIT

1. AppleTalk routing is disabled by default. To perform any AppleTalk routing configuration, you must first enable the feature. Select *AppleTalk Routing* from the Options menu.

2. Follow the onscreen instructions to enable AppleTalk Routing. The following menu will then be displayed:

```
AppleTalk Configuration Menu:

 1)  AppleTalk Routing (Enable/Disable)
 2)  AppleTalk Ports
 3)  AppleTalk Static Routes
 4)  AppleTalk Capacities
 5)  Isolated Mode (Enable/Disable)

Select function from above or <RET> for previous menu:
```

Note: AppleTalk routing can not be enabled unless hardware filtering is disabled.

USING MANAGE MODE COMMANDS

atalk

Displays the current AppleTalk Routing configuration.

APPLETALK ROUTING OPTION CONFIGURATION ELEMENT

APPLETALK OPERATIONAL STATUS

You can enable or disable the AppleTalk Routing option. When AppleTalk Routing is enabled, the CyberSWITCH acts as an AppleTalk Router, routing AppleTalk datagrams based on AppleTalk address information. When AppleTalk Routing is disabled, the CyberSWITCH will simply bridge AppleTalk protocol network traffic. By default, AppleTalk Routing is disabled.

APPLETALK ROUTING BACKGROUND INFORMATION

The CyberSWITCH supports the following AppleTalk protocols:

- Routing Table Maintenance Protocol (RTMP)
- Name Binding Protocol (NBP)
- Zone Information Protocol (ZIP)

Using these protocols, the CyberSWITCH AppleTalk Routing option allows remote LAN to LAN forwarding of AppleTalk datagrams.

When a datagram is to be forwarded to a remote site, the CyberSWITCH will initiate a circuit switched connection and forward the appropriate datagrams to that remote site. As the link utilization increases, the CyberSWITCH will make additional connections as required to provide a consistent level of performance to the device. As link utilization decreases, connections will be released.

APPLETALK PORTS

CONFIGURING APPLETALK PORTS

USING CFGEDIT

1. Select *AppleTalk Ports* from the AppleTalk configuration menu.

2. *Press 1* to add a port.

3. Select the type of port you are adding. Choices are LAN, WAN, WAN (UnNumbered), WAN (Mac Dial In), or WAN (Remote LAN).

4. Enter the user-defined port name.

5. For a LAN port only: enter the LAN port number.

6. Select the AppleTalk network type. Choices are extended or nonextended network.

7. Enter either the network range or the network number (depending on AppleTalk network type configured).
   - For extended networks: enter the range of AppleTalk network numbers. For the LAN port type, you may enter 0-0 to use the discovery mode.
   - For nonextended networks: Enter the AppleTalk network number. For the LAN port type, you may enter 0 to use the discovery mode.

   If the system is in the discovery mode, it is then a non-seed router, in which the system learns its configuration information from the seed router. Each network must have at least one seed router.

8. If you are configuring your system in the *nondiscovery* mode (you entered numbers other than 0 or 0-0 for the network range / number), complete the following:
   a. Enter either the suggested AppleTalk address or the suggested AppleTalk node Id (depending on AppleTalk network type configured).
      - For extended networks: enter the suggested AppleTalk address (includes the network number and the node's Id).
      - For nonextended networks: enter the suggested node Id.

      For the LAN port type, the address / node Id is optional. For the WAN port type, you must configure this information.
   b. Enter the zone name(s).
      - For extended networks, you may configure the network with multiple zones. You must enter a default zone name, then, if desired, you may enter additional zone names.
      - For nonextended networks, you may only configure one zone.

9. Return to the main AppleTalk Configuration Menu.

APPLETALK PORTS CONFIGURATION ELEMENTS

PORT TYPE

The type of physical network segment that the port connects to. The port type may either be *LAN*, *WAN*, *WAN UnNumbered, WAN (Mac Dial In)* or *WAN (Remote LAN)*.

- The *LAN* port type indicates that the system is physically connected to an Ethernet LAN segment.
- The *WAN* port type creates logical AppleTalk networks over WAN. It creates a logical AppleTalk network that comprises of multiple numbered point-to-point links with the same AppleTalk network range.
- The *WAN (UnNumbered)* port type also creates a logical AppleTalk network over WAN. It enables the system to use unnumbered point-to-point links.
- The *WAN (Mac Dial In)* port type allows multiple remote Macintosh devices to connect via numbered point-to-point links.
- The *WAN (Remote LAN)* port type allows remote bridge devices to connect to other AppleTalk router ports. The AppleTalk router then treats all bridge devices connected to the Remote LAN as if they were on an Ethernet LAN segment. All port parameters for the WAN (Remote LAN) port are the same as those of the WAN port type.

PORT NAME

A 1 to 16 character user-defined name that identifies the port to the system administrator.

LAN PORT NUMBER

For LAN port types only. This parameter indicates the port number of the Ethernet resource to which the physical LAN is connected.

APPLETALK NETWORK TYPE

The type of AppleTalk network that the port connects to. Possible network types are *Extended* and *NonExtended*.

- The *Extended Network* type indicates that the system is connected to an Extended AppleTalk network, which allows addressing of more than 254 nodes and supports multiple zones.
- The *NonExtended Network* indicates that the system is connected to a NonExtended AppleTalk network, which supports addressing of up to 254 nodes and supports only one zone.

APPLETALK NETWORK RANGE / NUMBER

The AppleTalk network range (for Extended network) or the AppleTalk network number (for NonExtended network) of the LAN segment that the port is connected to. Specifying 0.0 (for Extended) or 0 (for NonExtended) places the port in discovery mode (a.k.a., non-seed router), in which the system learns its configuration information from the seed router. Note that there must be at least one seed router on the network. Discovery mode is not supported for WAN ports, and therefore a valid network range / number needs to be specified.

SUGGESTED APPLETALK ADDRESS / NODE ID

If the system is acting as a seed router on this port, then this parameter specifies the suggested AppleTalk address (Extended) or Node Id (NonExtended), which is used as initial value for the AppleTalk address for the port. The default is no suggested address.

Note: An AppleTalk address consists of the network number followed by a node Id. For example, if the network number is 1234, and the node's Id is 56, the node's AppleTalk address would be 1234.56.

ZONE NAME(S)

The AppleTalk zone name(s) for the network that the port is connected to. For ports that are of the Extended network type, you *must* enter a default zone name, then you *may* enter any additional zones names. For ports that are of the NonExtended network type, you must configure one zone name, with no option to configure additional zone names.

APPLETALK PORTS BACKGROUND INFORMATION

THE APPLETALK NETWORK TYPE

An AppleTalk network consists of four basic pieces, the *nodes*, *networks*, *network numbers*, and *routers*. All these pieces together form an AppleTalk internet. Initial implementation of AppleTalk Phase 1 provided support for up to 254 nodes. Initially the need to have more than 254 nodes on an individual internet was not a concern, and the initial implementation worked fine.

As time passed, a need developed for more than 254 nodes on a network. As an answer to that need, AppleTalk Phase 2 was developed. Phase 2 introduced the fifth component to the AppleTalk internet, *network-number ranges*. An AppleTalk network that would continue to use a single network number would now be identified by a range of network numbers. Each of the network numbers in the range could support up to 253 nodes.

The Extended network type takes advantage of the network-number ranges produced by Phase 2, whereas the NonExtended network type does not use a range of network numbers.

DYNAMIC NODE ADDRESS ASSIGNMENT

Dynamic node address assignment is an addressing scheme that dynamically assigns node addresses rather than permanently associating an address with each node. This can save configuration time (for a LAN port, you are not required to enter an AppleTalk address / node Id), and also allows a node to move between networks without having to worry about addressing conflicts.

When a node joins the network, it assigns itself a node Id. It will send out a probe, to ensure that no other node on the network has the same Id. If you have configured a "suggested" AppleTalk address / node Id, that is the address / node Id the node includes in its probe.

THE ZONE CONCEPT

A zone is a logical group of nodes on an internet, much like the concept of subnetting with the world of IP. Within the framework of Phase 2 the logical assignment of zones is limited to 255 zone names for a network. Each name can be configured to represent a logical group within that respective internet. An example would be zone 1=Marketing, zone 2=Engineering etc. By configuring an AppleTalk router with logical zones you establish a mode of efficient data transport that acts much the same as IP with multiple subnets.

Although the concept of zones are the same as IP subnets, zone names do not have to be configured to encompass nodes with one physical location. Zones can be configured to incorporate nodes that are geographically diverse. Within this framework the dynamic address assignment allows the user to view all zones that are configured, and have been set up to give that particular user access to these zones. Thus, with this framework, a user can select the zone in which they want to be a part of for that particular task. Later, at a user's discretion, they may choose to be part of a different zone. If a user does not choose to associate with a respective zone, in a multi-zone internet a default zone is configured and all non-selective nodes will be associated with the default zone until a choice is made.

With the above in mind, continuing on with the ability to set up zones with non-local nodes, the network has an associated *zone multicast address*. When a device chooses a zone, it registers itself to receive packets sent to the specific zone-multicast address associated with that zone. Zone-multicast addresses are used to significantly reduce the overhead associated with dynamic naming.

APPLETALK REMOTE LAN

Overview

An AppleTalk WAN (Remote LAN) port connects remote bridge devices to other AppleTalk router ports. The AppleTalk router treats all bridge devices connected to the Remote LAN as if they were on an Ethernet LAN segment. That is, the CyberSWITCH emulates an Ethernet medium over the series of ISDN point-to-point connections. The AppleTalk router encapsulates AppleTalk data for the Remote LAN port in Ethernet packets and forwards the data to the remote bridges.

If the Remote LAN only has Macs connected to it, these Macs assume the AppleTalk network number / range assigned to the Remote LAN port. For these simple remote networks, you are not required to configure an AppleTalk network number for the remote bridge device. When the remote bridge connects, it is associated with the first configured AppleTalk Remote LAN port.

If the Remote LAN has both AppleTalk routers and Macs connected to it, the Macs assume the AppleTalk network number / range of the remote AppleTalk routers. For these remote networks, the AppleTalk Remote LAN network number / range must correspond to that of the remote AppleTalk router. In this case, you should configure an explicit AppleTalk network number for the remote bridge device so that the same network number is applied to the Remote LAN each time it connects. When the remote bridge connects, it is explicitly associated with the AppleTalk Remote LAN port that corresponds to the AppleTalk network number in the *bridge device table entry*.

Remote LAN ports differ from LAN ports on the handling of a configured network number / range versus a learned network number / range. LAN ports are by default soft seeds when a network number / range is configured. This means that if an RTMP packet is received with a different network number / range than configured, the LAN port assumes the RTMP packet contains the correct network / range and begins using the learned network number / range. If the network

number / range configured for the Remote LAN port differs from the network number / range that is being broadcasted in RTMP packets by other remote routers, the port becomes unusable.

Configuration

In order to properly set up an AppleTalk Remote LAN, you must:

- enable AppleTalk Routing from *Options*
- configure the WAN (Remote LAN) *port* from *Options, AppleTalk Routing, AppleTalk Ports*
- enable *bridging* and optionally specify an AppleTalk network number for the pertinent device level entries from *Security, Device-Level Databases, On-node Device Entries*

Considerations

Note the following in regard to the AppleTalk Remote LAN feature:

- The CyberSWITCH does not initiate connections to AppleTalk Remote LAN devices. The remote bridge is responsible for connecting to the CyberSWITCH. The CyberSWITCH can forward packets to the remote device once a connection is established.
- AppleTalk spoofing is not currently supported for this feature.
- Off-node route lookup is not currently supported for this feature.

APPLETALK STATIC ROUTES

CONFIGURING APPLETALK STATIC ROUTES

USING CFGEDIT

1. Select *AppleTalk Static Routes* from the AppleTalk Routing Menu.

2. *Press 1* to add a static route.

3. Select the AppleTalk network type of the destination network.

4. Enter the destination network range / number reachable through this static route.

5. Enter the AppleTalk address of the Next Hop device, or, enter "0.0" if the Next Hop device is over an unnumbered link.

6. If you entered "0" for the AppleTalk address of the Next Hop device, enter the device name of the Next Hop device. (Note that the device information for the Next Hop device must be already configured. Refer to *Configuring a On-node Device Database* for instructions for configuring device information.)

7. Enter the number of hops for this route.

8. Enter the zone name(s) of the remote network.
   For an extended network, there will be a default zone name, and there will possibly be additional zone names.

   For nonextended networks, there will be a single zone name.

APPLETALK ROUTING STATIC ROUTES CONFIGURATION ELEMENTS

APPLETALK NETWORK TYPE
The AppleTalk network type used by the destination network of this static route. Type can be either *Extended Network* or *NonExtended Network*.

DESTINATION NETWORK RANGE / NUMBER
The remote AppleTalk network range (for Extended network) or network number (for NonExtended network) reachable through this static route entry.

NEXT HOP DEVICE
The AppleTalk address of the next hop device that provides access to the destination AppleTalk network. If the next hop is over an unnumbered WAN link, then the device name is specified. The name must be a valid Device table entry.

NUMBER OF HOPS
The number of AppleTalk routers that are traversed in order to reach the destination AppleTalk network.

ZONE NAME(S)
The name of the zone(s) on the remote AppleTalk network.

APPLETALK ROUTING STATIC ROUTES BACKGROUND INFORMATION

You only need to configure static routing entries if you need to access a WAN network that is not directly connected to the system, or if you need to access a LAN network through a router that does not support AppleTalk RTMP. Static routes specify the AppleTalk address of the next hop router that provides access to this network.

APPLETALK CAPACITIES

CONFIGURING APPLETALK CAPACITIES

USING CFGEDIT

1. Select *AppleTalk Capacities* from the AppleTalk Routing Menu.

2. Press 1 to set the maximum number of entries for the AppleTalk Route table.

3. Press 2 to set the maximum number of entries for the AppleTalk zone table.

APPLETALK CAPACITIES CONFIGURATION ELEMENTS

APPLETALK ROUTING TABLE MAXIMUM NUMBER OF ENTRIES
Allows you to set the maximum number of defined and learned routing table entries. The default value is 512. The maximum is 2,000.

APPLETALK ZONE TABLE MAXIMUM NUMBER OF ENTRIES
Allows you to set the maximum number of defined and learned zone table entries. The default value is 512. The maximum is 2,000.

APPLETALK CAPACITIES BACKGROUND INFORMATION

This option allows you to control the maximum number of table entries (routing and zone tables) for your network.

APPLETALK ISOLATED MODE

CONFIGURING THE APPLETALK ISOLATED MODE

USING CFGEDIT

1. Select *Isolated Mode* (*Enable/Disable)* from the AppleTalk Routing Menu.

2. Follow the onscreen instructions to either enable or disable the isolated mode.

APPLETALK ISOLATED MODE CONFIGURATION ELEMENTS

ISOLATED MODE STATUS
You may enable or disable the AppleTalk Isolated Mode. When operating with the isolated mode enabled, the system does not relay AppleTalk datagrams received from the WAN to other AppleTalk devices located on the WAN. AppleTalk datagrams received on the LAN port are forwarded to each required port.

The Isolated Mode is disabled by default. This is the appropriate configuration for almost all devices.

CONFIGURING CALL CONTROL

OVERVIEW

The CyberSWITCH offers a number of configurable options to control how the system will make and accept calls. These options, each of which are described in this chapter, include:

- configuring throughput monitor parameters
- configuring call interval parameters
- configuring monthly call charge parameters
- configuring call restriction parameters
- configuring bandwidth reservation parameters (including device profiles)
- configuring semipermanent connection parameters
- configuring Connection Services Manager (CSM) as a Call Control Manager
- configuring D Channel Callback for devices authenticated by CSM
- configuring modem inactivity timeout parameters

Note: This chapter does not describe the configuration of call detail recording (CDR) information. Refer to *Log Options* in the *Configuring Advanced Options* chapter for this configuration.

CALL CONTROL MENU

To begin the configuration of any of the call control options using CFGEDIT, follow these steps:

1. Select *Options* from the main menu.

2. Select *Call Control Options* from the options menu. This will display the following call control menu:

```
Call Control Options Menu:

   1)  Throughput Monitor
   2)  Call Intervals
   3)  Monthly Call Charges
   4)  Call Restrictions
   5)  Device Profile Options
   6)  Bandwidth Reservation
   7)  Semipermanent Connection
   8)  CSM as Call Control Manager
   9)  D Channel Callback
   10) Digital Modem Inactivity Timeout

Select function from above or <RET> for previous menu:
```

THROUGHPUT MONITOR

CONFIGURING THE THROUGHPUT MONITOR

Notes: Throughput Monitoring parameters do not apply to Digital Modems. Refer to the *Digital Modem Inactivity Timeout* feature for an alternative.

Certain restrictions apply to the use of the *Throughput Monitor and Semipermanent Connections*. Refer to the Background Information.

USING CFGEDIT

1. Select *Throughput Monitor* from the Call Control Options menu.
2. The current throughput monitor configuration will be displayed. Enter *Y* to change the configuration.
3. Follow the onscreen instructions to keep the feature enabled.
4. Enter the sample rate in seconds.
5. Enter the overload trigger number.
6. Enter the overload window size.
7. Enter the overload percentage utilization.
8. Enter the underload trigger number.
9. Enter the underload window size.
10. Enter the idle trigger number.
11. Enter the idle window size.
12. Enter the idle percentage utilization.
13. Press "Y" to accept the configuration changes you have made.

USING MANAGE MODE COMMANDS

`thruput`
Displays the current throughput monitor configuration data.

`thruput change`
Allows the current throughput monitor configuration data to be changed. Refer to the CFGEDIT section for specific parameters.

THROUGHPUT MONITOR CONFIGURATION ELEMENTS

SAMPLE RATE
A Sample Rate identifies the number of seconds for each sample period. The default setting for the sample rate is 5 seconds. During this period, the system keeps track of the total number of bytes that is transferred in both directions between two systems. The utilization percentage is determined by comparing this total with the realistic maximum for the current aggregate amount of bandwidth.

OVERLOAD TRIGGER NUMBER
The number of samples within the window that must exceed the specified utilization for the OVERLOAD condition to occur.

OVERLOAD WINDOW SIZE
The number of sample periods (up to 32) that you should use as the sliding window.

OVERLOAD PERCENT UTILIZATION
The percentage of the available bandwidth that the traffic samples must exceed for an overload condition to occur.

UNDERLOAD TRIGGER NUMBER
The number of samples within the window that must be below the next lowest target capacity for the UNDERLOAD condition to occur.

UNDERLOAD WINDOW SIZE
The number of sample periods (up to 32) that you should use as the sliding window.

IDLE TRIGGER NUMBER
The number of samples within the window that must be below the specified utilization for the IDLE condition to occur.

IDLE WINDOW SIZE
The number of sample periods (up to 32) that you should use as the sliding window.

IDLE PERCENT UTILIZATION
The percentage of available bandwidth on the last connection that traffic samples must fall below for the connection to be considered IDLE.

Note: The system monitors for the IDLE condition when only one connection to a site exists, and that connection is a switched connection.

THROUGHPUT MONITOR BACKGROUND INFORMATION

A powerful feature of the CyberSWITCH is its ability to add and drop calls depending on the amount of WAN traffic. If no information is being sent, the call will be terminated. The system will also make additional calls to a site if it is determined that extra bandwidth is needed.

The Bandwidth Management feature works by sampling the amount of data that is transmitted and received on the connections between two units. Each sample is compared to the levels associated with the different conditions. The results of these comparisons are kept in a sliding window. The window size, number of samples that trigger an event, and sampling frequency are configurable.

The default Throughput Monitor configuration will work for initial installation. These parameters can be changed to better match the bandwidth needs of your location.

Correctly tuning these parameters is important in order to eliminate unnecessary data calls. The default value for the sample rate is a 5 second sample period. The following chart provides the default values for the remaining throughput monitoring parameters.

Condition	*Trigger Number*	*Window Size*	*Utilization*
Overload	6	12	90%
Underload	12	24	---
Idle	32	32	1%

Note: For adding calls, these parameters only apply to calls initiated by the system.

The throughput monitor feature constantly monitors the use of the connections and looks for the following conditions:

- The overload condition, which indicates that demand exceeds the current aggregate capacity of the WAN connections. The system can add more bandwidth when this occurs.
- The underload condition, which indicates that demand falls below a target capacity that is lower than the current aggregate capacity. The system can release any previously added bandwidth when this occurs.
- The idle condition, which indicates that the last connection remaining is no longer needed.

The following sections explain each of these conditions in greater detail. Following the condition explanations, a throughput monitoring example is provided for further clarification.

OVERLOAD CONDITION MONITORING

The overload condition is monitored by comparing the samples to an upper threshold. The sample is marked as a true condition if either the transmit or the receive byte count exceeds the threshold. When the number of true samples in the window reaches the configured limit, the overload condition has occurred.

The overload threshold is configured as a utilization percentage of the aggregate bandwidth for a group of connections between two Systems.

If the system determines that the bandwidth can be increased, it will add a new channel into the connection group. At this time, the system adjusts its upper threshold for the new aggregate capacity and resets its counters. If the new capacity still cannot satisfy the transmit demand, the system will again detect the overload condition.

Similarly, when bandwidth is decreased, the system will remove a channel from the group of connections. The system adjusts its threshold accordingly, resets its counters, and begins monitoring for the overload condition against the lower aggregate capacity.

UNDERLOAD CONDITION MONITORING

The underload condition is monitored by comparing the samples with a lower threshold. The sample is marked as a true condition if both the transmit and the receive byte count fall below the threshold. When the number of true samples in the window reaches the configured limit, the underload condition has occurred.

The purpose of detecting this condition is to decide if connections can be released. Therefore, an underload threshold is defined in terms of a target bandwidth that is less than the current aggregate bandwidth. The underload condition indicates that the target capacity can satisfy the traffic demand.

When only one circuit remains in a group, the underload mechanism determines if a lower bandwidth circuit would satisfy the demand. For example, if one 384Kbps circuit remained, a target of 64Kbps could be specified and the above described mechanisms will identify when the 64Kbps circuit would satisfy the demand.

IDLE CONDITION MONITORING

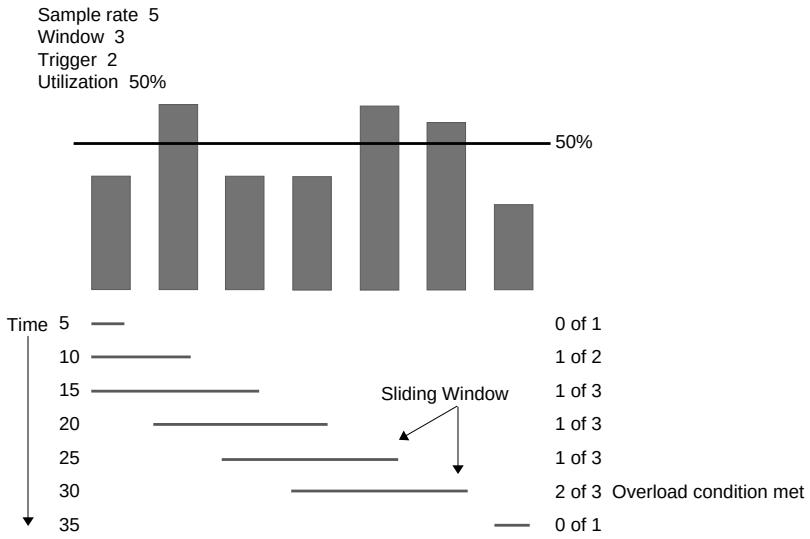
The CyberSWITCH monitors for the idle condition when only one connection to another site remains. The system detects when there is no longer a need to maintain connectivity with the other site. An absolute idle condition is defined as a number of consecutive sample periods with zero bytes transferred.

Keep-alive type frames may sometimes continue to flow when there is no actual device data flowing. The system would not detect a completely idle condition, and might leave a connection in use when it may no longer carry useful traffic. Instead of monitoring for zero traffic, the idle condition can be set up to detect extremely low, but non-zero, bandwidth utilization. This can be done by not requiring all samples in the window to be zero, or by monitoring for a low percentage utilization level.

Background traffic is often transmitted continuously. It may be necessary to have a minimum dedicated connection to handle the constant traffic, then use switched connections for peak loads and backup.

THROUGHPUT MONITOR CONFIGURATION EXAMPLE

In the following example, the sample rate is 5 seconds, the number of samples to examine per sample rate (the window) is 3, the configured percentage to compare against (utilization) is 50 percent, the number of times the sample's utilization percentage must be greater than the configured utilization percentage (the trigger) is 2 out of 3 samples. To make things simpler for this example, there is only one call up and we are only checking to add another call (overload).



After 5 seconds the sample is checked and the average utilization for the 5 seconds was 40 percent. This is less than the configured utilization percentage of 50%, so no action is taken. For the second sample rate period, the average throughput is 60%. This percentage is greater than the configured utilization percentage, so the trigger must also be checked. At this point, only 2 samples have been taken, and the configured window is for 3 samples. The overload condition needs to be met 2 times (the trigger of 2) out of 3 samples (the window of 3) before any action is taken. This condition has not been met.

The average throughput is 40% for the third sample rate period. This is less than the configured utilization, so out of the last 3 samples (a sliding window is in use), 1 out of 3 samples have throughput that is greater than the configured utilization. The overload condition has still not been met. No extra calls are made.

After the fourth sample rate period (20 seconds have now passed), the first sample is dropped. The average throughput for the new sample is below the configured utilization percentage. Therefore, 1 out of 3 samples have throughput that is greater than the configured utilization. No extra calls are made.

After the fifth sample period, the second sample taken is dropped. The average throughput for the new sample taken is 60%. But because the sample dropped was a sample that was greater than the configured utilization, there still are only 1 out of 3 samples that are greater than the configured utilization.

After the sixth sample period, the third sample taken is dropped. The average throughput for the new sample is over the configured utilization. The trigger then has been met; two out of three samples have met the overload condition. An extra call will be added, and the process will be reset.

CALL INTERVAL PARAMETERS

CONFIGURING THE CALL INTERVAL PARAMETERS

USING CFGEDIT

1. Select *Call Intervals* from the Call Control Options menu.
2. Enter the minimum time interval between call attempts.

CALL INTERVAL CONFIGURATION ELEMENTS

MINIMUM TIME INTERVAL
The configured call interval is the minimum time between call attempts. The system will not make a call attempt in less than the configured call attempt value. However, due to the system hardware clock resolution, the actual time interval may be greater than the configured value. The default value is 0.70 seconds. The range of the configured value is 0 to 5 seconds, in 1/100 second increments. A configured value of 0 implies that the system will make call attempts without any delay between them.

CALL INTERVAL BACKGROUND INFORMATION

This parameter allows the configuration of the minimum interval between call attempts. This interval applies to the entire system, including all lines, sites, and devices.

The Call Interval is configured in terms of hundredths of seconds. The default value is .7 seconds. The range of the configured value is 0 to 5 seconds. A configured value of 0 implies that the system will make call attempts without any delay between them.

The default value of .7 seconds is compliant with the Communications Industries Association of Japan's(CIAJ) regulation. This regulation states that no customer premise equipment should make more than 3 call attempts within 2 seconds. This prevents certain model switches from being overloaded. In areas where these low capacity switches are not installed, calls can be made more frequently.

Before the system initiates a data connection, it first checks the time at which the last connection was initiated. If the time from the last connection attempt to the new connection attempt is less than the configured call interval, the new connection is placed on an outgoing call queue. The queue is then serviced at the configured call interval.

MONTHLY CALL CHARGE

CONFIGURING MONTHLY CALL CHARGE

USING CFGEDIT

1. Select *Call Charges* from the Call Control Options menu.
2. Follow the onscreen instructions to enable this feature.
3. Enter the maximum monthly charge you would like to set (specified in Yen for NTT connections).
4. Select the action to take if the maximum is exceeded.

MONTHLY CALL CHARGE CONFIGURATION ELEMENTS

STATUS
Allows you to enable or disable the monthly call charge option.

MAXIMUM MONTHLY CHARGE
The maximum monthly charge value. The legal values are from 1 to 10,000,000. This value is specified according to the country's currency.

ACTION
Select the action to be taken if the maximum monthly call charge is exceeded. The Stop Calling action will cause the system to stop initiating switched calls. Dedicated connections and incoming calls will continue to operate normally. The continue calling action will cause the system to continue making calls even after the maximum monthly charge is exceeded.

MONTHLY CALL CHARGE BACKGROUND INFORMATION

Currently, this feature is only supported on connections to NTT, NET5, and 1TR6 switches. The "Advice of Charge" information element delivered by the switches are required to track phone call charges.

When the Monthly Call Charges option is enabled, phone call charges are tracked by the system. If the total call charges exceed this configured maximum during the month, the configured action will be taken. At the beginning of a new month, the current total call charges will be reset to 0.

The LCD panel displays the current total call charges for the month. If the configured maximum call charges are exceeded, the system reports a message and the configured action is taken. Refer to the *LCD Messages* chapter for a listing of the associated LCD messages.

CALL RESTRICTIONS

CONFIGURING CALL RESTRICTIONS

Note: Certain restrictions apply to the use of *Call Restrictions and Semipermanent Connections*. Refer to the Background Information discussion.

USING CFGEDIT

1. Select *Call Restrictions* from the Call Control Options menu.
2. Follow the onscreen instructions for enabling this feature.
3. The current call restriction configuration will be displayed.
4. Enter the number Id associated with the parameter you want to change.
5. Follow the onscreen instructions for changing the parameter.

USING MANAGE MODE COMMANDS

`alarm`
Displays the current status of the audible alarm. It is displayed as either enabled or disabled. If enabled, the audible alarm will sound when a call restriction condition has been met.

`alarm off`
Disables the audible alarm that sounds when a call restriction condition has been met.

`alarm on`
Enables the audible alarm that sounds when a Call Restriction condition has been met.

`callrest`
Displays the current Call Restriction configuration data.

`callrest off`
Disables the Call Restriction feature.

`callrest on`
Enables the Call Restriction feature.

CALL RESTRICTION CONFIGURATION ELEMENTS

STATUS
Allows you to enable or disable the call restriction option.

HOURS CALLS ARE ALLOWED
The allowable hours for outbound calls (inbound calls will always be allowed). Separate each hour by a comma. Ranges are allowed by inserting a dash (-) between the first and last hours in the range. A zero entered by itself will allow no calls during any hour.

Two actions are available if an outbound call is attempted at any other time:

1. The call will not be allowed; a message will be displayed on the LCD, and written to the report log.

2. The call will be allowed; however, a warning will be displayed on the LCD and written to the report log.

The following chart provides the numbers you should use to represent the am and pm hours of the hours calls are allowed:

From: *To:*	*12:00* *12:59*	*1:00* *1:59*	*2:00* *2:59*	*3:00* *3:59*	*4:00* *4:59*	*5:00* *5:59*	*6:00* *6:59*	*7:00* *7:59*	*8:00* *8:59*	*9:00* *9:59*	*10:00* *10:59*	*11:00* *11:59*
am hour	1	2	3	4	5	6	7	8	9	10	11	12
pm hour	13	14	15	16	17	18	19	20	21	22	23	24

The following chart provides example entries for hours calls are allowed:

Hours Calls Allowed	*Entry*
8am to 5pm	9-18
all hours	1-24
10am to 6pm, 8pm, 11pm	11-19, 21, 24
8am to 5pm, 7pm to 9pm	9-18, 20-22

MAXIMUM CALLS PER DAY
Allows you to limit the number of calls made per day by configuring a maximum number of calls. The default value is 300 calls per day. Statistics will be logged to track the total number of calls made per day. This statistic will be written to the statistics log every half hour, and will be available through the *ds* command. The current value of this statistic will be displayed on the LCD, and also will be displayed on the monitor when the *cr stats* command is used.

Two actions are available if this maximum is exceeded:

1. The call will not be allowed; a message will be displayed on the LCD, and written to the report log.

2. The call will be allowed; however, a warning will be displayed on the LCD, and written to the report log.

MAXIMUM CALLS PER MONTH
The maximum number allowed per month. The default value is 6900 calls per month. Statistics will be logged to track the total number of calls made per month. This statistic will be written to the statistics log every half hour, and will be available through the *ds* command. The current value of this statistic will be displayed on the LCD, and will also be displayed on the monitor when the *cr stats* command is used.

Two actions are available if this maximum is exceeded. These actions are:

1. The call will not be allowed; a message will be displayed on the LCD, and written to the report log.

2. The call will be allowed; however, a warning will be displayed on the LCD, and written to the report log.

CALL MINUTES PER DAY
The limit of number of call minutes per day. The default value is 240 call minutes per day. Call minutes will be calculated periodically while calls are active (not when a call is disconnected). Statistics will be kept to track the total number of call minutes made per day. This statistic will be written to the statistics log every half hour, and available through the *ds* command. The current value of this statistic will be displayed on the LCD. It will also be displayed on the monitor when the *cr stats* command is used.

Two actions are available if this limit is exceeded. These actions are:

1. The call will not be allowed; a message will be displayed on the LCD, and written to the report log.

2. The call will be allowed; however, a warning will be displayed on the LCD, and written to the report log.

Note: Existing calls will not be disconnected when this limit is reached. Subsequent calls may not be allowed, but existing calls will be allowed to continue.

MAXIMUM CALL MINUTES PER MONTH
The maximum number of call minutes per month. The default value is 5520 call minutes per month. Call minutes will be calculated periodically while calls are active (not when a call is disconnected). Statistics will be kept to track the total number of call minutes made per month. This statistic will be written to the statistics log every half hour, and available through the *ds* command. The current value of this statistic will be displayed on the LCD, and will also be displayed on the monitor when the *cr stats* command is used.

Two actions are available if this limit is exceeded. These actions are:
1. The call will not be allowed; a message will displayed on the LCD, and be written to the report log.
2. The call will be allowed; however, a warning will be displayed on the LCD, and written to the report log.

Note: Existing calls will not be disconnected when this limit is reached. Subsequent calls may not be allowed, but existing calls will be allowed to continue.

MAXIMUM CALL LENGTH
The maximum amount of time (in minutes) that a call is allowed to be active. The default value is 240 minutes.

Note: The system checks for violation of configured maximum call length every five minutes. So, for example, if you set the maximum call length to one minute, there will be a five minute window around that one minute in which the system will check for a violation.

Two actions are available if a call exceeds this limit. These actions are:

1. The call is disconnected; a message will be displayed on the LCD, and written to the report log.

2. The call is continued; however, a warning will be displayed on the LCD, and written to the report log.

AUDIBLE ALARM STATUS
The audible alarm can be enabled or disabled. This alarm is used to signal you when a call restriction has been violated. The alarm is a series of beeps, that are repeated every 5 minutes while any call restriction is in violation.

CALL RESTRICTIONS BACKGROUND INFORMATION

The Call Restriction feature provides the ability to place limits on the toll costs of operating the CyberSWITCH. Call Restriction consists of a variety of features that can restrict the number of switched calls made to remote sites, and also limit the amount of call minutes accumulated for remote site access.

Notes: It is important to note that the Call Restriction feature only applies to outbound calls from the system.

When a condition occurs that triggers a warning to be written to the log, the message will be written only once for the duration of the condition.

For example, if the network's total amount of connect time is estimated to be less than three hours per day, call restrictions could be set up to place a limit on the number of call minutes per day to 240. (Three hours would be 180 minutes; however, there may be some unusual days that go over a little, hence, 240 minutes.) If a newly installed application starts sending out packets on the LAN that causes remote connections to be made all the time, the system will terminate the call, and prevent any more calls from being made after 4 hours (240 minutes) of connect time to the remote site. Thus, the phone bill would be limited to just four hours of connection time. If desired, the system can be configured to issue a warning when the limit is exceeded instead of stopping the calls.

BANDWIDTH RESERVATION

The bandwidth reservation feature allows a portion of possible CyberSWITCH connections to always be available to specific devices for both inbound and outbound calls.

CONFIGURING BANDWIDTH RESERVATION

To implement this feature, you need to configure specific device profiles, reference them in the device list, and then enable the bandwidth reservation feature. These three steps are described in detail in this section.

USING CFGEDIT

To configure a specific device profile:

1. Select *Options* from the main menu.

2. Select *Call Control Options* from the options menu.

3. Select *Device Profiles* from the Call Control Options Menu. The following screen is then displayed, showing the default device profile:

```
Current Device Profiles:

id Profile NAME         LINES (SLOT,PORT)
-------------------------------------------------------------------
1   Default_Profile     (1,1 1,2 1,3 1,4)

(1) Add, (2) Change, (3) Delete a Profile or press <RET> for previous menu:
```

Note that there are four lines in the default profile: (1,1), (1,2), (1,3), and (1,4). The leading "1" in the pair of numbers represents the slot number. The second number in the pair represents the port number. This example shows that there is only one BRI adapter, and it is installed in slot number one, and has four ports. There is a line for each port number.

4. Press 1 to add a device profile.

5. Enter a user-defined unique name to identify the profile. We will use Central_Site for our example profile name. The following screen will then be displayed:

```
Profile NAME = Central_Site

is currently allowed access to:
id      Line          id      Line
----------------------------------------
      No Lines Configured

(1) Add new line, (2) Delete Line or press <RET> for previous menu?
```

6. Press 1 to add a new line. This will assign a line to the profile you are configuring.

7. The screen will show all data lines that were previously configured. Follow the prompts to enter the slot number and port number of the line you are reserving for this profile.

8. You may continue adding new lines for this profile, or press <RET> to exit this menu sequence.

Notes: Listing or adding a line under a profile doesn't, by itself, *reserve* the line for devices with that profile. Listing the line simply means that devices with that profile are allowed to use the line. To *reserve* a line, you must guarantee that the line is listed for a unique profile only. In other words, no lines are reserved for a profile unless that line is assigned to that profile AND also unassigned to all other profiles.

Adding a device profile does not affect the default profile. You may want to consider deleting the lines you are reserving for your profile from the default profile. To delete the reserved lines from the default profile, press 2 at the *Device Profile* screen to change a profile. Follow the on-screen instructions to delete a line from the default profile. This will reserve the line for a specific device and no one else.

To reference the specific device profile in the device list:

Assigning a specific device profile to a device will give that device usage of the line you configured in the above section. To assign a specific device profile to a device you need to enter the device profile information when you are configuring the device's ISDN information. You may either configure the device profile information when you are first adding the device, or you may add the information later. To enter the profile information:

1. Select "3" from the main menu to configure security.

2. Select "3" from the Security Menu to configure device level database information.

3. Select "2" from the Device Level Databases Menu to configure on-node device database entries.

4. If this is a new device, follow the onscreen instructions to add a device. If this is a previously configured device, select the device Id for the device for which you will add a device profile.

5. Under ISDN information, enter the profile information. This is a profile name you configured in the previous section. Remember from the previous section that each configured profile reserves specific lines. By assigning this profile to the device, you are reserving specific lines for this device.

To enable the bandwidth reservation feature:

1. Return to the Options Menu (selection 2 of the main menu).

2. Select *Bandwidth Reservation*.

3. Follow the onscreen instructions to enable the feature.

USING MANAGE MODE

profile
Displays the current profile table.

profile [add] [change] [delete]
Allows you to add, change or make deletions from the current profile table.

bwres [on] [off]
System-level command which enables/disables the bandwidth reservation feature.

device [add] [change] [delete]
Allows you to assign a device to a profile.

BANDWIDTH RESERVATION CONFIGURATION ELEMENTS

DEFAULT PROFILE
The Default Profile is the available profile for all valid devices not identified with a specific device profile. The Default Profile initially contains all of the BRI lines configured in the Physical Resources section of CFGEDIT. When data lines are added, changed or deleted through CFGEDIT's Physical Resources section, they are automatically added, changed or deleted in the Default Profile.

The Default Profile entry cannot be deleted, nor have its name changed. However, it may be modified to remove lines from general usage.

DEVICE PROFILE
The Device Profile entry identifies which line or lines are reserved for a particular profile. The profile name must be a string of 1 to 17 alphanumeric characters, including the underscore. When selecting a name for a Device Profile, select a name that appropriately identifies the profile (such as Central Office).

LINE
This element identifies the line or lines to be reserved for the specified Device Profile. Overlap of lines between profiles is allowed. Note that this is a BRI-only feature since bandwidth is reserved per-line.

BANDWIDTH RESERVATION BACKGROUND INFORMATION

This feature allows a portion of the possible connections to always be available to specific devices for both inbound and outbound calls. To increase flexibility, this feature may be configured to either allow or prevent bandwidth overlap. Bandwidth overlap will allow normal devices to use a certain number of lines, while a special class of super devices would be allowed access to both the normal bandwidth (designated in the default profile) as well as special super device bandwidth (designated in the configured device profile). "No overlap" would restrict each set of devices to their own lines.

When configuring your bandwidth reservation, consider the following:

- This is a BRI-only feature since bandwidth is reserved per-line.
- It is necessary to reject calls from devices who have mistakenly called in on a line reserved for other device(s).
- Outbound calls are also restricted to the lines reserved for a device.
- When Bandwidth Reservation is disabled, any device will can connect on any line.
- When Bandwidth Reservation is enabled, a default profile list of lines will be configured for use by all devices that are not configured to use an alternate profile in the reserved list. This default profile list may be configured to remove lines from general use.

SEMIPERMANENT CONNECTIONS

A semipermanent connection is a connection that is up at all times. With semipermanent connections, one or more switched calls are made at system start-up, and are kept up until system shutdown. This feature minimizes the number of calls which the system makes, and maximizes the number of active call minutes.

Every device can have one semipermanent connection. Each semipermanent connection is composed of one or more calls. The number of semipermanent devices is limited to the maximum number of calls allowed by the system.

CONFIGURING SEMIPERMANENT CONNECTIONS

Note: The *initial data rate* for both sides of the connection must either be configured identically or the throughput monitor feature must be turned off for the remote side of the connection.

USING CFGEDIT

1. Select *Options* from the main menu.
2. Select *Call Control Options* from the Options menu.
3. Select *Semipermanent Connections* from the Call Control Options menu.
4. Press 1 to add a semipermanent connection.
5. Enter the device name to associate with the connection as shown below:

```
Enter the name of the device to add to the semipermanent device list
or <RET> to cancel menu: Mike Mason
```

6. Determine if the CyberSWITCH should always retry a call. If yes, then configuration for the device is done, the device is entered into the semipermanent device list, and appears as shown below. If no, continue to step 7.

```
Semipermanent Connections Menu:

 id   Device Name                Max Retries   Over Interval   Session Interval
------------------------------ ------------ -------------- ------------------
  1   "Mike Mason"                      (ALWAYS CALL BACK)

(1) Add, (2) Change, (3) Delete a Semipermanent Connection
or <RET> for previous menu:
```

7. Enter the maximum number of times to retry a call.

8. Enter the time interval during which the CyberSWITCH keeps track of disconnects.

9. Determine if the CyberSWITCH should attempt to retry a call after a rejection. If yes, continue to step 10. If no, then configuration for the device is done, the device is entered into the semipermanent device list, and appears as shown below.

```
Semipermanent Connections Menu:

 id   Device Name                Max Retries   Over Interval   Session Interval
------------------------------ ------------ -------------- ------------------
  1   "Mike Mason"                   10             10 Mins              N/A

(1) Add, (2) Change, (3) Delete a Semipermanent Connection
or <RET> for previous menu:
```

10. Enter the time interval before a call is retried. The device is entered into the semipermanent device list, and appears as shown below.

```
Semipermanent Connections Menu:

 id   Device Name                Max Retries   Over Interval   Session Interval
------------------------------ ------------ -------------- ------------------
  1   "Mike Mason"                   10             10 Mins           60 Mins

(1) Add, (2) Change, (3) Delete a Semipermanent Connection
or <RET> for previous menu:
```

USING MANAGE MODE COMMANDS

semiperm

Displays the semipermanent connection menu. The configuration screens are identical to those displayed by CFGEDIT. Refer to the above section for instructions.

semiperm [add] [change] [delete]

Adds, changes, or deletes a semipermanent connection from the current configuration.

SEMIPERMANENT CONNECTIONS CONFIGURATION ELEMENTS

DEVICE NAME
Specify the device name (from the Device List) that you wish to make a semipermanent connection. Once specified, the semipermanent feature will (at least) keep the Initial Data Rate active to the specified device, as long as it is not prohibited by call restrictions or a physical or configuration problem. The number of semipermanent devices is limited to the maximum number of calls the CyberSWITCH supports.

MAX RETRIES
The maximum number of times the CyberSWITCH will retry a call in the Over Interval time period. The default is 10.

OVER INTERVAL
The time period in minutes during which the CyberSWITCH will keep track of the number of disconnects. For example, a disconnect will occur if the device fails authentication. The timer begins when the first disconnect occurs, and if the timer expires without reaching the maximum number of disconnects, the disconnect counter is rest. Otherwise, if the maximum number of disconnect is reached, then the device is moved to the rejected state. The default is 10 minutes.

SESSION INTERVAL
The time period beginning when the device enters the rejected state. When the timer expires, the device is returned to the trying state and the CyberSWITCH attempts to connect to the device. The default is 60 minutes. "N / A" appears when the CyberSWITCH will not attempt a call again after a rejection.

Note: When the Session Interval is configured, a device can fail authentication, move to the rejected state, move back to the trying state after the timer expires, and fail authentication again. This cycle can repeat an infinite number of times, depending on the status of call restrictions. The CyberSWITCH will not stop this cycle until a call restriction limit his reached or it is overridden by the system administrator by issuing the *`disc device`* command.

SEMIPERMANENT CONNECTIONS BACKGROUND INFORMATION

In many areas, ISDN is tariffed by call, and not by connect time. This feature is ideal for areas like this. Semipermanent connections allow you to automatically make a connection at startup time, and keep that connection up at all times.

Although semipermanent connections are up at all times, they are different from dedicated connections. A dedicated connection is simply a Layer 1 pipe for data. A semipermanent connection is one or more switched calls made at startup and kept until shutdown.

The sections below provide information concerning how semipermanent connections interact with other system features.

INTERACTIONS WITH OTHER FEATURES

Call Device Commands

Issuing the *`call device`* or *`disc device`* commands will effect the semipermanent connection. These commands will override the semipermanent connection.

Call Restrictions

You may wish to disable call restrictions when using semipermanent connections. Call restrictions are mainly intended for use in areas where "per minute" ISDN tariffs are in place. Typically, this in not the case if semipermanent connections are in use.

If you decide not to disable Call Restrictions, we recommend that you make the following Call Restriction parameter alterations:

- Change the maximum call duration to warn only.
- Add 1,440 minutes to the Call Minutes per Day for every call in a configured semipermanent connection.
- Add 43,200 minutes to Call Minutes per Month for every call in a configured semipermanent connection.
- Allow calls for all hours in the day.

Refer to the instructions for changing the *parameter values*.

Throughput Monitor

The semipermanent connection feature, along with the throughput monitor, interact to prevent the CyberSWITCH from dropping calls which are part of the semipermanent connection.

However, specific considerations apply to the use of the Throughput Monitor. Consider these two situations:

1. To connect two systems together with semipermanent connections:
   For each system, configure a semipermanent connection to the other, and enable Throughput Monitoring on both.

   However, you may occasionally see a "glare" condition (i.e., both machines attempting to reestablish the connection after a network or power outage). This "glare" condition will not occur if the semipermanent connection utilizes the entire bandwidth available at either system site. Normal throughput monitoring will drop the extra call if traffic allows.

   If this glare condition is unacceptable, you may either:
   - Delete all Dial-Out phone numbers (through CFGEDIT, Device List entries) for one of the sites. The other site (that still has Dial-Out configured) will then create the semipermanent connection.
   - Treat one system as a device which does not support semipermanent connections. (See item 2, which follows).

2. To connect an system to a machine that does not support semipermanent connections, disable Throughput Monitoring at the remote device.

If neither of these options are used, the remote device may periodically drop calls which are members of a semipermanent connection. The semipermanent connection feature will stop making calls if the number of connections dropped reaches the maximum within configured time limit. If this happens, you will need to use the `call device` command to restart the feature.

CSM AS A CALL CONTROL MANAGER

This feature allows you to use the CSM for call control management only. This feature allows you to continue to use other authentication servers (e.g., RADIUS, ACE) yet still gain the benefits of CSM call control management.

CONFIGURING CSM FOR CALL CONTROL

USING CFGEDIT

1. Select *CSM as Call Control Manager* from the Call Control Options menu.
2. The current status of the CSM Call Control Server will be displayed. Select 1 to toggle between enabled and disabled, and ensure an *enabled* setting.
3. Select *TCP port number* if you wish to change this setting. Changes here will also appear on the CSM Authentication menu.
4. Return to the *Main Menu*.
5. For authentication, if you are using the *On-node Device Table* or *Off-node Device Level Security*, you are finished with the configuration of this feature. If you are using *User Level Security*, you may wish to adjust the Authentication Time-out and/or change the Call Control Failure banner. Continue with the following steps.
6. Select *Security* and then *Network Login Information*.
7. Select *Network Login General Configuration*.
8. Select *Authentication Timeout*. Follow on-screen instructions to adjust this value.
9. Return to the Network Login Information Menu and select *Network Login Banners*.
10. Select the *Call Control Failure Banner*. Follow on-screen instructions to adjust this banner.

Note: If you are using CSM as your authentication manager, you do not have to configure the call control option separately. This is only necessary when you are configuring another device for authentication, and wish to use CSM for call control only.

CONFIGURATION ELEMENTS

STATUS
Allows you to enable or disable CSM for call control management.

TCP PORT NUMBER
The TCP port number used by CSM. Note that you can assign a user-defined port number, but that the CSM TCP port number must be entered identically on both the CyberSWITCH and CSM.

AUTHENTICATION TIMEOUT TIMER
This timer represents the amount of time the CyberSWITCH will wait for the Authentication Agent to handle a login attempt before timing out. If CSM is enabled as Call Control Manager, this time-out value must then represent the amount of time for both:

- the Authenticating Agent to respond to the login attempt, *and*
- CSM to respond to the login attempt.

CALL CONTROL FAILURE BANNER
If CSM does not permit call connectivity for any reason, the CyberSWITCH will display the message "CSM Denied Access". You may change this default message to whatever you choose through this configuration element.

BACKGROUND INFORMATION

Cabletron's CSM consists of an administration program and a user interface, and runs with a database and a standard SQL server. It acts as both an authentication server and call control manager for the CyberSWITCH. This product is described in detail in the *CSM User's Guide* which accompanies the product.

If you are interested in call control management without CSM authentication, the *CSM as Call Control Manager* is now an available feature. This feature provides call control management with any authentication agent (e.g., RADIUS, ACE, TACACS).

To use CSM for call control management only, you must enable the feature. The call will be authenticated through the chosen method, and then call control management will pass to CSM. Acceptable authentication methods are:

- RADIUS at device level
- CSM at device level
- RADIUS at user level
- ACE at user level
- TACACS at user level
- On-node Device Table at device level

In all cases, the device information is propagated into the CyberSWITCH from the authentication agent. (This implies that IP static routes and IP pooling are configured on the CyberSWITCH, and not CSM.) When CSM is not the authenticating agent, CSM cannot initiate outgoing calls. To make outgoing calls from the CyberSWITCH, you must use other means of initiation, based on type of security (e.g., IP route lookup using RADIUS).

CALL CONTROL MANAGEMENT

CSM call control management varies depending upon the type of security in use:

- Device Level Security
  If you use the On-node Device Table as authentication agent, CSM merely logs call start and end times. (You do not need to configure devices in the CSM database).

  If you use an off-node authentication server for authentication: configure devices on CSM as well. This will provide access to the following CSM call control management features: call restrictions, maximum bandwidth, and grouping (in addition to the call logging feature).
- User Level Security

If you use user level security for authentication: configure devices on CSM as well. This will provide access to the following CSM call control management features: call restrictions, maximum bandwidth, and grouping (in addition to the call logging feature).

User level security and CSM call control management work together as follows: CSM allows a device to connect under an alias name until the user can be verified by its authentication server. Once the user is properly authenticated, the device's name is forwarded to the CSM. CSM can then further determine whether or not the device should be allowed connectivity at this time.

Possible reasons CSM may disconnect the device's call:
- Call restrictions reached for this device.
- Maximum bandwidth reached for this device.
- Device and CyberSWITCH to which it is connected are not part of the same group.
- Device on a reserved channel and not a reserved device.
- Device not defined in CSM.

Note: The alias assigned to initial calls is *REMOTEx*. Be sure you do not use this name for any of your device names when configuring CSM or your authentication server.

LIMITATIONS/CONSIDERATIONS

- CSM must not initiate outgoing connections through the CyberSWITCH using non-CSM authentication.
- CSM as Call Control Manager may not be disabled if CSM is the authentication agent.
- CSM as Call Control Manager is not disabled when CSM as authentication agent is disabled.
- CSM does not override information found on the authenticating server except for: call restrictions, maximum bandwidth, and grouping.
- CSM does not allow device names of *REMOTEx* to be configured.

D CHANNEL CALLBACK

This feature allows the CyberSWITCH to use the calling ID from the D channel on an incoming ISDN call to identify a device using CSM, reject the incoming call, and call the device back. By doing this, all phone charges can be incurred by the central site rather than the remote sites.

Note: This option is only available if you are using CSM for device level authentication. Also, callback is currently implemented for only PRI NET5 and BRI NI1 switch types. Other switch types will be added later.

Modem callback is also available. No CyberSWITCH configuration changes are necessary. All configuration changes are made through CSM for modem callback. Refer to CSM user documentation for configuration instructions and to CyberSWITCH documentation for verification procedures.

CONFIGURING D CHANNEL CALLBACK

USING CFGEDIT

1. From CFGEDIT's *Options* Menu, select *Call Control Options*.
2. Select *D Channel Callback.*

3. The current status D Channel Callback will be displayed. Select 1 to toggle from *disabled* to *enabled* (as shown by the following screen).

```
D Channel Callback Menu:

                                          Current Settings
   1)  D Channel Callback (Enable/Disable)      Enabled

Select function from above or <RET> for previous menu:
```

Note: In addition to the CFGEDIT configuration changes, you must also do some configuration through CSM for callback to work. You must define the calling device on CSM. For each configured calling device make sure to:

- Configure a calling line ID for the number the device will be using when calling into the CyberSWITCH (located under the device's *Telephone* tab).
- Configure the telephone number to be used to call back to the calling device (located under the device's *Telephone* tab). This number is often the same as the CLID or possibly with a preceding 9 if under Centrex.
- Enable the Callback option (located under the device's *Access/Other* tab).
- Enable Outbound Authentication if you want to make sure the device you are calling back to is the correct device (located under the device's *Access/Authentication* tab).

For more detailed instructions, refer to the CSM user documentation.

USING MANAGE MODE COMMANDS

There are no associated Manage Mode commands.

D CHANNEL CALLBACK CONFIGURATION ELEMENTS

CALLBACK STATUS
You may select to enable or disable the callback feature for devices using CSM for authentication.

D CHANNEL CALLBACK BACKGROUND INFORMATION

When an incoming ISDN call is presented to the CyberSWITCH, certain information is presented on the D Channel including the callers telephone number. Rather than accept the call right away, the CyberSWITCH uses the calling line ID (CLID) to send a request to CSM to do a lookup based on this CLID (as noted earlier, this option is only available if you are using CSM for device level authentication). If CSM can find a device which has a matching CLID configured and that device has callback enabled, we will reject the call being presented and wait for CSM to issue a call request to the device previously identified. If callback is NOT enabled in CSM for this device or NO device could be identified by this CLID, we will allow the call presented to be accepted and will proceed to the authentication phase using PAP/CHAP/ etc. as usual.

DIGITAL MODEM INACTIVITY TIMEOUT

This feature allows the CyberSWITCH to disconnect inactive modem connections based on lack of activity for a specified amount of time. This feature does not affect digital HDLC connections.

CONFIGURING THE DIGITAL MODEM INACTIVITY TIMEOUT

USING CFGEDIT

1. From CFGEDIT's *Options* Menu, select *Call Control Options*.
2. Select *Digital Modem Inactivity Timeout*. A screen similar to the following will display:

```
The Modem Inactivity Timeout is currently DISABLED.

Do you wish to change the Current Modem Inactivity Timeout Configura-
tion (Y or N)  [default = N]:   ?   Y

Do you wish to ENABLE the Modem Inactivity Timeout (Y or N) [default
= N]:  ?   Y

Modem Inactivity Timeout  (1 - 42 minutes)  [default = DISABLED]:  ?
30
```

3. Respond to the menu prompts to change the current configuration, and then enable the Modem Inactivity Timeout feature.
4. Specify, in minutes, the amount of time the CyberSWITCH should wait to terminate connections to inactive digital modem devices.
5. To activate the new Modem Inactivity Timeout value, you must save CFGEDIT changes, and restart the CyberSWITCH.

USING MANAGE MODE COMMANDS

modinact
Displays the current Modem Inactivity Timeout value.

modinact [change]
Allows you to change the Modem Inactivity Timeout configuration as if you were in the CFGEDIT screen.

Note: If this feature is changed using Manage Mode, the changes will not affect any calls currently up or in progress. It will only affect subsequent calls.

MODEM INACTIVITY TIMEOUT CONFIGURATION ELEMENTS

MODEM INACTIVITY TIMEOUT VALUE
The amount of time, in minutes, the CyberSWITCH should wait before terminating connections to digital modem devices based on a lack of data transfer. You may specify a value between 1 and 42 minutes. The default value is 0 (feature disabled).

MODEM INACTIVITY TIMEOUT BACKGROUND INFORMATION

The Modem Inactivity Timeout feature allows the CyberSWITCH to terminate connections to digital modem devices based on a lack of data transfer for a specified amount of time. This feature applies to both incoming and outbound calls.

The Modem Inactivity Timeout feature supports DM-24, DM-24+ and DM-30+ modem adapters only, on CyberSWITCH systems running UAA software release 7.3 or beyond. The feature is not supported for DM-8 adapters. When you configure a value for the Modem Inactivity Timeout, that value will then apply to all qualified modems resident on the CyberSWITCH.

Unlike the *Throughput Monitor*, any activity whatsoever (transmitted or received) will keep a call up and restart the Modem Inactivity Timer. If you wish to limit the duration of calls regardless of traffic, use *Call Restrictions* or *CSM Manager*.

CONFIGURING OTHER ADVANCED OPTIONS

OVERVIEW

This chapter provides information for configuring advanced system options that are not covered in the previous chapters. These options include:

- configuring for a Digital Modem
- configuring default async protocol
- configuring PPP
- configuring default line protocol
- configuring log options
- configuring system compression options
- configuring TFTP
- configuring file attributes

THE DIGITAL MODEM

In addition to ISDN support, the CyberSWITCH becomes an analog modem pool through its Digital Modem feature. The Digital Modem feature consists of both hardware and software elements to support up to 30 K56Flex modems (handling 300 bps to 56 Kbps) on a *single adapter*. This adapter is connected to an ISDN BRI or PRI adapter via an intercard bus. This Digital Modem adapter performs the modulation or demodulation and Async-Sync conversions, as necessary. The system then sends the data to the LAN.

The Digital Modem feature allows the system to accommodate both incoming and outgoing analog calls (i.e., it can receive and initiate connections). The feature conforms to the V.90 standard (which supports K56Flex), and will support connections from remote modems that also conform to this same standard.

CONFIGURING FOR A DIGITAL MODEM

USING CFGEDIT

1. Configure basic system configuration, including the configuration of resources and lines (See *Configuring Resources).* Note that when you configure the Digital Modem resource, you must specify whether the resource is a DM-8, DM-24, or a DM-30. You do not need to distinguish between V.34+ and K56Flex modems; the CyberSWITCH will do this internally.

2. Select and configure protocol. The digital modem may use:
   - IP Routing
   - IPX Routing
   - AppleTalk

   For *IP routing*:
   a. Make sure IP routing is enabled.
   b. Configure the LAN interface to represent local IP Network that may receive and send datagrams (refer to the *Configuring Interfaces* in the *Configuring Basic IP Routing* chapter).
   c. Configure the WAN or WAN Direct Host interface to represent remote networks that may receive and / or initiate calls (refer to the *Configuring Interfaces* in the *Configuring Basic IP*

Routing chapter). Note that Digital Modem does not support WAN RLAN or WAN unNumbered interfaces.

For *IPX routing*:

a. Make sure IPX routing is enabled.
b. Configure the LAN interface to represent local IPX Network that may receive and send datagrams (*Configuring IPX* chapter).
c. Configure the WAN interface to represent remote networks that may receive and / or initiate calls. Note that Digital Modem does not support WAN Remote LAN interfaces.

For *AppleTalk routing*:

a. Make sure AppleTalk routing is enabled.
b. Configure the AppleTalk ports to represent the AppleTalk Network that may receive and send datagrams (*Configuring AppleTalk* chapter). Note that Digital Modem does not support unnumbered WAN interfaces. For WAN interfaces, do not assign a port number.

3. Increase the login time-out value to 45 or 50 seconds to accommodate the Digital Modem (*Configuring Default Line Protocol*).

4. Select and configure *Default Async Protocol*. You may specify your default to be PPP protocol or Terminal Mode. PPP protocol allows for the transfer of async PPP data; terminal mode provides remote analog console access.

5. Select *Call Control Options*, and then *Digital Modem Inactivity Timeout*. Configure the amount of time, in minutes, you want the CyberSWITCH to wait before disconnecting an inactive connection.

6. Configure the Device List entries for all remote modem type devices (*Configuring Device Level Databases* chapter).

Note: You must properly set up your application at the remote site as well. Follow the steps outlined below:

At the remote site (with analog modem):

1. Reflect the same IP address as the WAN or WAN Direct Host Interface.

2. Configure login.

3. Configure password.

DIGITAL MODEM BACKGROUND INFORMATION

The Digital Modem feature offers an ISDN device the ability to use analog modems to initiate calls to the CyberSWITCH. The Digital Modem feature provides network access to telecommuters, mobile computer users, and other analog-modem users in remote areas not yet serviced by ISDN.

The Digital Modem feature consists of both hardware and software elements. The hardware consists of a separate adapter which includes up to 24 V.34+ modems or 30 K56Flex modems. It handles traffic from 300 bps to 56 Kbps.

The Digital Modem software identifies, directs, and converts the data stream appropriately. For example, if an incoming call to the system is identified as coming from an analog modem, the associated ISDN B-channel is routed to the Digital Modem adapter. Software assigns it to one of the digital modem modules, and all of the operations of a V.34+ or K56Flex modem are performed just as if the call had gone to an analog modem through an analog phone line. The data is demodulated, and then sent to an internal Asynchronous Usage Discriminator (AUD), which monitors the data stream. This AUD determines if the caller wishes to use PPP protocol, or whether it is requesting remote analog console access. This determination is made within a configurable time frame:

- if the *AUD detects four carriage returns* from the caller, it will provide the caller with remote analog console access by presenting the caller with a CyberSWITCH login prompt.
- if the *AUD detects PPP LCP frames*, it connects the caller to a PPP stack. An Async-PPP-to-Sync-PPP conversion is performed, and then the system sends the data to the LAN as appropriate.
- if the *AUD does NOT detect* the PPP LCP frames nor the carriage returns, it will still attempt to send the data to the PPP stack.

The Digital Modem feature supports the following features:

- auto speed detection and negotiation
- auto step down and step up during session if line is noisy
- up to 56 Kbps modem speed (backwards compatible down to 300 baud)
- data compression which is automatically negotiated (with maximum 4:1 compression, up to 115.2 Kbps DTE speed)
- error control

These features are also dependent upon the analog modem you are using, since the features must be supported by both devices in order to be operable.

Refer to the following chapters for more information: *Hardware Overview*, *Hardware Installation* and *System Adapters Appendix*. Refer to the *Digital Modem Commands* section for methods to display active connections, display or erase digital modem statistics, add or delete individual modems, and upgrade modem firmware when necessary.

SUPPORTED MODES OF CONNECTION

The Digital Modem supports either a PPP mode or terminal mode type of connection.

In PPP mode, the Digital Modem uses Asynchronous Point-to-Point Protocol (Async-PPP) as its link protocol. Therefore, the system with Digital Modem will support remote devices attached by modem that provide Async-PPP dial-in. This protocol is very popular for analog modem networking, and is built into many leading remote application programs. Modem connectivity is not provided for RFC 1294 devices or HDLC Bridge devices.

For authentication, the remote device must support either PAP and/or CHAP.

In addition to Async-PPP, the CyberSWITCH supports a terminal-mode type of connection. This mode provides the opportunity for remote user-level authentication before Async-PPP data transfer, or it provides the opportunity for remote analog console access. For more information, refer to *Terminal Mode* in the *Default Async Protocol* section.

RELATIONSHIPS BETWEEN DIGITAL MODEM AND OTHER FEATURES

Note the following:

- RADIUS Authentication: Authentication is performed before the call is routed to the Digital Modem Adapter. Once the call is validated, the call is routed to the Digital Modem Adapter to establish a modem link.
- Throughput Monitoring: Overload and Underload conditions do not apply, since the Digital Modem feature only uses one B-channel per call. However, the Idle condition (in which the system releases an idle call after a certain length of time) is still valid. Since this condition may not be as important to analog calls as it would be to ISDN calls, you may want to set this threshold higher than the default. You may do so using the Manage Mode command: `thruput change.`
- Concerning the `cs`, `mc` and `cdr` commands: the data rate displayed for Digital Modem calls will be the actual transmit rate from the CyberSWITCH's perspective. If no rate is reported by the modem, then the value will default to 64K.

DEFAULT ASYNC PROTOCOL

The default async protocol option applies to digital modem applications only. It allows you to specify default values for the CyberSWITCH when handling incoming asynchronous calls. The configurable options include:

- *PPP Mode*: for standard async-PPP data transfer. This mode assures that the digital modem connects the caller to a PPP stack, performs an async-PPP-to-sync-PPP conversion, and then sends the data to the LAN as appropriate.
- *Terminal Mode*: provides a means for user-level authentication before PPP data transfer, or provides remote analog console access for system management.
- *Call Disconnect*: automatically disconnects call if no data received within the configured data time-out duration.

When an incoming connection is established to the CyberSWITCH, system software "autosenses" the type of connection. It looks at the first few bytes of received data and determines whether the connection is terminal mode or PPP mode. If no data is received within a configurable amount of time, the system takes action based on the configured default parameter. A description of the configuration of this default parameter follows.

PPP MODE

USING CFGEDIT

To set the default to PPP mode:

1. From *Options*, select *Default Async Protocol*.
2. Select *Action on Data Timeout*.
3. Select *Use PPP Protocol*.
4. Next, select *Data Timeout Value*. Change value, in seconds as desired (minimum: 1; maximum: 60).

USING MANAGE MODE

`termopt`

Allows you to change the default async protocol configuration as if you were in the CFGEDIT screen.

TERMINAL MODE

USING CFGEDIT

1. From *Options*, select *Default Async Protocol*.
2. Select *Action on Data Timeout*.
3. Select *Use Terminal Mode*.
4. Next, select *Data Timeout Value*. Change value, in seconds, as desired (minimum: 1; maximum: 60).
5. Return to Main Menu and select *Security*.
6. Select *Network Login Information*.
7. Select *Network Login General Configuration*.
8. Select *Terminal Server Security*:
   a. To default to remote analog console access for system management, select *Use Administrative Login*.
   b. To default to user-level authentication before PPP transfer, select the authentication server you plan to use. Your choices are: *RADIUS*, *TACACS* and *ACE*. In addition, you must also configure the remaining security options to support user-level authentication. Refer to *Security Overview* (and its related chapters) for more information.
   c. If you want the default to be no terminal access when time has expired, select *Do not allow terminal access*.

USING MANAGE MODE

`termopt`
Allows you to change the default async protocol configuration as if in CFGEDIT screen.

CALL DISCONNECT

USING CFGEDIT

1. From *Options*, select *Default Async Protocol*.
2. Select *Action on Data Timeout*.
3. Select *Disconnect*.
4. Next, select *Data Timeout Value*. Change value, in seconds, to the amount of time you want the system to wait before disconnecting (maximum: 60 seconds).

USING MANAGE MODE

`termopt`
Allows you to change the default async protocol configuration as if in CFGEDIT screen.

DEFAULT ASYNC PROTOCOL CONFIGURATION ELEMENTS

ACTION ON DATA TIMEOUT
Determines the action the CyberSWITCH will take when it receives no data during the autosense mode and time has expired. Configurable values are: *Disconnect*, *Use PPP Protocol*, and *Use Terminal Mode*. The default is *Disconnect*.

If no data is received within the data timeout duration, the following events will occur:

- If *Disconnect* is configured, the CyberSWITCH will disconnect the call.
- If *Use PPP Protocol* is configured, the CyberSWITCH will assign the call to a PPP subsystem.
- If *Use Terminal Mode* is configured, the CyberSWITCH will assign the call to the terminal I/O subsystem and/or the user-level authentication server.

DATA TIMEOUT VALUE

Determines how long (in seconds) the CyberSWITCH will wait to receive data during autosense mode. If the configured time expires, the CyberSWITCH will take configured action for the connection. The minimum value is 1 second; the maximum value is 60 seconds. The default is 30 seconds.

Note: This timer starts at the beginning of a call and includes the time for the modems to negotiate (typically 10-12 seconds). Be sure to allow for this additional time to avoid the *Action on Data Timeout* before negotiation is completed.

After terminal-user authentication, this timer restarts. The CyberSWITCH returns to autosense mode again and if no data received, the user will need to reauthenticate.

TERMINAL SERVER SECURITY

Specifies which type of user-level authentication server to use for terminal mode connections. The selections are: *RADIUS*, *TACACS*, *ACE*, *Use Administrative Login* or *Do not allow terminal access*. The *Use Administrative Login* value will present terminal users with a normal CyberSWITCH admin login prompt. The *Do not allow...* value will not permit terminal access upon data timeout and will disconnect the call. The default is *Do not allow terminal access*.

BACKGROUND INFORMATION

This feature supports the ability to handle terminal mode connections via dial-up client software packages, such as *WIN95 Dial-up Networking*. Terminal mode connections are useful for authenticating remote modem users via user-level authentication, then providing PPP protocol data communications. It also provides a means of system management using a remote console. For X.25 users, it provides remote modem users a means of access to different X.25 services.

When an incoming connection is established to the CyberSWITCH, system software *autosenses* the type of connection. The system looks at the first few bytes of received data and determines whether the connection is terminal mode or PPP mode. If no data is received within a configurable amount of time, the system takes action based on one of the following configured parameters:

- *PPP Mode*: normal CyberSWITCH authentication and data forwarding procedures apply to this connection
- *Terminal Mode*: connection processed by CyberSWITCH I/O subsystem which handles character-oriented data. Connection assigned to user-level authentication task. Authentication process proceeds per configured user-level authentication parameters and method of operation.

  If authentication fails, the connection is released as per the configured authentication parameters.

  If authentication succeeds, the authentication task completes its functions such as displaying the message of the day. Once authenticated, control passes to a PPP subsystem and the connection enters PPP mode. Device-level authentication and protocol stream handling proceeds per configured device information.

Note: If the CyberSWITCH is configured for PPP Mode, the caller at the remote device can override this through manual intervention. The caller must initiate four carriage returns upon call connection to notify the system that the caller requests console access. (These CRs must take place within the time specified in the data timeout value).

AUTOSENSE FEATURE

When the CyberSWITCH receives an incoming call, it doesn't know what type of device is at the remote end. The CyberSWITCH uses an autosense feature to determine the type of connection. This feature looks at the first few bytes of received data to determine connection type. If data matches a known protocol id, the CyberSWITCH enters PPP mode for that connection. If the received data does not match a known protocol id and is displayable ASCII characters, the CyberSWITCH enters terminal mode for that connection.

LIMITATIONS

Note the following limitations concerning Terminal Mode connections:

- supported on asynchronous types of connections via a digital modem connection
- cannot use SLIP protocol
- requires device + user-level security configuration (in *System Security*)
- can use RADIUS for user-level authentication but not device authentication
- Terminal mode users must have a device entry configured in either the on-node device database or Connection Services Manager (CSM). This entry may be configured manually or *dynamically*.
- All terminal mode connections must use the same off-node user-level authentication.
- There is a maximum of 8 simultaneous user-level authentication sessions, which include Terminal Mode and Telnet authentication sessions.

INTERACTIONS WITH OTHER FEATURES

Authentication and Call Control:

- *User-level authentication*: The user-level authentication process is used on all terminal mode connections.
- *Device-level authentication*: If device-level security is desired in addition to user-level security, the device name (on-node or CSM) must match the login id provided in user-level authentication. Also, the user name and password in the dial-up networking configuration on the PC client must match the device name and password / secret configured on-node or in CSM. Finally, the Outbound Authentication flag in the device configuration must be set to *enabled*. If Outbound Authentication is set to disabled, only the user-level authentication will take place for the terminal mode connection.

  Note: Even if you do not wish to use device-level authentication, you must still configure a device entry for terminal mode users. This entry will provide the CyberSWITCH with important protocol information concerning the terminal mode connection.
- *CSM Call Control*: If call control by CSM is desired, a device matching the user-level authentication login id must be configured in CSM. This is true even if there is already an on-node device entry for this user.

PPP CONFIGURATION

CONFIGURING PPP

Note: A thorough understanding of PPP protocol is required before you attempt to change the PPP configuration. By changing the PPP configuration, you are changing the PPP protocol negotiation parameters. These parameters only need to be changed when you are attempting to interoperate with devices that do not provide a standard PPP implementation. Changing these parameters can result in PPP option negotiation failure and the inability to communicate with remote devices. The default parameters are adequate for most sites.

USING CFGEDIT

1. Select *PPP Options* from the options menu.

2. Change the Global PPP options.
   a. Change the max terminate value.
   b. Change the max configure value.
   c. Change the max failure value.
   d. Change the restart timer value.

3. Change the LCP configuration options.
   a. Change the LCP protocol field compression (PFC).
   b. Change the LCP address control field compression (ACFC).

4. Change the IPCP configuration options.
   a. Change the IPCP IP address negotiation initiation.

5. Change the Link Failure Detection Options.
   a. Enable or disable the link failure detection feature.
   b. Set the echo frequency.
   c. Configure the maximum attempts.

PPP CONFIGURATION ELEMENTS

MAX TERMINATE
The number of Terminate-Request packets sent without receiving a Terminate-Ack before assuming that the peer is unable to respond.

MAX CONFIGURE
The number of Configure-Request packets sent without receiving a valid Configure-Ack, Configure-Nak or Configure-Reject before assuming that the peer is unable to respond.

MAX FAILURE
The number of Configure-Nak packets sent without sending a Configure-Ack before assuming that configuration is not converging. Any additional Configure-Nak packets are converted to Configure-Reject packets.

RESTART TIMER
Times transmissions of Configure-Request and Terminate-Request packets. Expiration of the Restart timer causes a Timeout event, and retransmission of the corresponding Configure-Request or Terminate-Request packet.

LCP PROTOCOL FIELD COMPRESSION (PFC)
Provides a way to negotiate the compression of the Data Link Layer Protocol field.

LCP ADDRESS CONTROL FIELD COMPRESSION (ACFC)
Provides a way to negotiate the compression of the data link layer address and control fields.

RECEIVE SETTINGS
The receive settings for PFC and ACFC control whether (and how) the system receives PPP Packets with PFC or ACFC. Receive setting options include:
- mandatory: requested, repeated indefinitely if NAK'd
- preferable: requested, repeated up to MaxAttempts times if NAK'd
- supported: not requested, a peer request will be ACK'd
- not supported: not requested, NAK'd if the peer requests it

SEND SETTINGS
The send settings for PFC and ACFC control whether (and how) the system sends PPP packets with PFC or ACFC. Send setting options include:
- mandatory: requested, repeated indefinitely if NAK'd
- preferable: requested, repeated up to MaxAttempts times if NAK'd
- supported: not requested, a peer request will be ACK'd
- not supported: not requested, NAK'd if the peer requests it

IPCP ADDRESS NEGOTIATION INITIATION
IPCP address negotiation initiation defines when IPCP will initiate “IP address” IPCP option negotiation. The possible choices are:
- always initiate: IPCP will always initiate the IP address option negotiation (on a PPP link).
- If IP Address Unknown: IPCP will initiate the negotiation only when the peer’s IP address is unknown (for example, the system is running in the no-security mode, or the device entry does not have an IP address configured.

Note: The default value is “Always Initiate.”

LINK FAILURE DETECTION STATUS
You can enable or disable the link failure detection feature. If enabled, there will be a periodic transmission of Echo-Request frames, a maintenance type frame provided by PPP’s Link Control Protocol. Reception of the appropriate Echo-Reply frame indicates a properly functioning connection; incorrect replies or lack of replies indicate a connection failure.

ECHO FREQUENCY
This specifies, in seconds, how often the Echo-Request frames are transmitted (see above element). The default value is 10 seconds.

MAXIMUM ATTEMPTS
This specifies how many consecutive Echo-Requests are sent without receiving a reply before declaring the PPP link to be faulty. The default value is 3 attempts.

PPP Background Information

Point-to-Point Protocol (PPP) can provide standard interoperability for remote devices. Interoperability will allow remote devices made by different manufacturers to operate and exchange information on the same network.

PPP consists of three main parts:

1. A method of encapsulating datagrams so that they can be more easily transmitted over point-to-point links.

2. A Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection.

3. A family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols.

Link Control Protocol (LCP) is used to:

- automatically agree upon the encapsulation formation options
- handle the varying limits on sizes of packets
- authenticate the identity of the remote device on the link
- determine when a link is functioning properly
- detect common misconfiguration errors
- terminate the link

After a link is established through LCP, the Network Control Protocols (NCPs) manage the specific needs required by each device's network-layer protocol.

PPP Link Failure Detection

On a point-to-point link, there are a variety of failures which can occur on the intervening communications path and / or within the remotely connected system. Often times, such failures are detectable via a signalling mechanism associated with the link. For example, a failure of an ISDN B-channel usually leads to a corresponding failure of the associated D-channel, an event which is suitable for concluding that the B-channel has failed. Similarly, the Local Management Interface (LMI) facility of a Frame Relay circuit may provide feedback suitable for determining that an end-to-end Virtual Circuit has failed.

However, the PPP link exists on an end-to-end basis with the remote peer, a domain which exceeds that controlled by the signalling-type entities just cited. Thus, not every end-to-end failure will be detected. Some examples of such failures include:

- an ISDN peer's D-channel "process" is functional, but it's B-channel "process" has failed
- the underlying physical circuit has an end-to-end fault in one or both directions which does not affect the D-channel or control path
- the underlying physical circuit has been mistakenly looped back

In such cases, the Link Failure Detection feature can discern the fault(s). A properly functioning remote device is obligated to return an Echo-Reply to each Echo-Request, which verifies the full end-to-end path of the point-to-point link. Furthermore, the Echo-Request frames carry a PPP element known as the "Magic Number" which can be used to ascertain if an inbound Echo-Request truly came from the peer or was looped back.

PPP Link Failure Detection can be enabled or disabled within the PPP Options configuration menu. When enabled, two other configurable parameters then control the mechanism. Upon entrance of a PPP link into Network Phase (the point at which device data transfer is allowed), Echo-Requests will be sent at a configured frequency. As long as Echo-Replies are received, the link is deemed to be functional.

A second parameter specifies the maximum number of Echo-Request attempts which will be transmitted without a reply. If this limit is reached, a message is logged and the link is reported as faulty. Thus, the configured frequency multiplied by the configured maximum attempts yields the approximate time it will take to detect a failed link.

Note: Within the CyberSWITCH, there are certain accesses which also present the ability to enable / disable the periodic transmission of link maintenance type packets. For example, the packet-based Frame Relay access supports the configurable enable / disable of "Keepalives" in order to avoid the extra per-packet costs which the periodic Echo-Request frames might incur. The PPP Link Detection Failure feature will honor such access-based configuration, in addition to the explicit enable / disable configuration status of the PPP feature itself.

PPP REFERENCE DOCUMENTS

Point-to-Point Protocol (PPP) is also described in more detail in the set of RFCs listed below:

- RFC 1661 The Point-to-Point Protocol
- RFC 1638 PPP Bridging Control Protocol (BCP)
- RFC 1549 PPP in HDLC Framing
- RFC 1547 Requirements for an Internet Standard Point-to-Point Protocol
- RFC 1334 PPP Authentication Protocols
- RFC 1332 The PPP Internet Protocol Control Protocol (IPCP)

DEFAULT LINE PROTOCOL

The default values for this feature are adequate for most situations. Instructions are included for the rare instance that you need to alter the configuration.

Note: This feature does not apply to analog connections (including digital modem).

CONFIGURING DEFAULT LINE PROTOCOL

USING CFGEDIT

1. Select *Default Line Protocol* from the Options menu.
2. Change the action on the frame timeout.
3. Change the frame timeout value.

USING MANAGE MODE

lineprot
Displays the current default line protocol configuration.

lineprot change
Allows you to change the default line protocol configuration. For the configuration steps, refer to the previous CFGEDIT section.

DEFAULT LINE PROTOCOL CONFIGURATION ELEMENTS

ACTION ON FRAME TIMEOUT
The action to be taken if no frame is received before the configured frame timeout value has expired. The default value is to disconnect the call. The complete list of choices is as follows:

- Disconnect
- Use HDLC Bridge Protocol
- Use IP Host Protocol (RFC 1294)
- Use PPP Protocol

FRAME TIMEOUT VALUE
The time limit to wait to receive a packet. The default frame timeout value is 30 seconds. The possible range is from 5 to 60 seconds.

DEFAULT LINE PROTOCOL BACKGROUND INFORMATION

When a connection occurs, the system waits for a packet to arrive, and from that packet, it determines the protocol type. After a default frame timeout value of 30 seconds, if no packet is received, the default action on frame timeout is to disconnect the call.

It is possible to change the timeout value for waiting for responses. You may also change the action on frame timeout. Instead of disconnecting after the frame timeout value has been reached, you can select a default protocol for the system to use.

LOG OPTIONS

Log options allow you to direct log reports (call detail recording, system message reports, or authentication message reports) to a specific location. Reports can be directed to a local log file, or to a UNIX-style Syslog Server.

CONFIGURING LOG OPTIONS

USING CFGEDIT

1. Select *Log Options* from the Options menu. A menu similar to the following will be displayed:

```
Log Options Menu:

   1) Log Servers
   2) Call Detail Recording
   3) System Message (DR) log
   4) Authentication Message (DA) log

Select function from above or <RET> for previous menu:
```

2. Configure a Syslog Server:
   a. Select *Log Servers*. (Note that upon selection, no configuration is needed for a local log file. The local log file name is preconfigured.)
   b. Select *Add a Syslog Server*.
   c. Enter the Syslog Server IP address using dotted decimal notation.
   d. Enter the UDP port number for the Syslog Server.
   e. Return to Log Options Menu.

3. Identify which reports should be sent to which server:
   a. From *Log Options*, select *Call Detail Recording*.
   - Press <1> to select an active server to which the CDR log reports should be sent.
   - From the displayed list, enter the ID of the log file you wish to use.
   - Enter the decimal UNIX priority value.

   b. From *Log Options*, select *System Message (DR) log*.
   - Press <1> to select an active server to which the System Message log reports should be sent.
   - From the displayed list, enter the ID of the log file you wish to use.
   - Enter the decimal UNIX priority value.

   c. From *Log Options*, select *Authentication Message (DA) log*.
   - Press <1> to select an active server to which the Authentication Message log reports should be sent.
   - From the displayed list, enter the ID of the log file you wish to use.
   - Enter the decimal UNIX priority value.

USING MANAGE MODE COMMANDS

`log options`

Displays the Log Options menu. The configuration screens are identical to those displayed by CFGEDIT. Refer to the above section for instructions.

LOG OPTIONS CONFIGURATION ELEMENTS

Note: The local log file path and file name is preconfigured for your system; no configuration elements are entered for a local log file. Configuration elements are only needed for Syslog Servers.

IP ADDRESS

The IP address of the Syslog Server using dotted decimal notation; 0.0.0.0 and 255.255.255.255 are not allowed. The Syslog Server must be accessible via a LAN connection (and not a WAN connection).

UDP PORT
The default port number is "514", which should work for most installations. Consult your UNIX documentation if you are unsure of the UDP port number.

DECIMAL UNIX PRIORITY VALUE
The default priority value is "38", which should work for most installations. (Refer to *Syslog Server* description, or consult your Server documentation if there are any problems). This value is prepended to all messages sent to the Syslog Server; it is used by the Syslog Server to determine how to handle the log message.

SYSLOG SERVER
You may select to send reports to a Syslog Server rather than the local log. In the *Call Detail Recording Menu*, *System Message (DR) log Menu*, and *Authentication Message (DA) log Menu*, add a Syslog Server to the list of active servers to indicate that CRD and/or System and Authentication Message reports should be sent to that server.

Note: You do not have to configure a Syslog Server name. The first Syslog Server configured will be automatically named Syslog1, the second Syslog2, and so on. Up to ten Syslog Servers can be configured. (For storing CDR reports, you can select up to three of these servers.)

LOG OPTIONS BACKGROUND INFORMATION

The Log Options feature expands the system's log file capability and provides a consistent interface to the device when working with logging or tracing the activity of a subsystem. Currently, the log options feature supports *call detail recording* (CDR), *system message* (DR) and *authentication message* (DA) subsystems.

The log reports that allow you to trace the activity of a subsystem can be directed to a specific location. The reports can be directed to a *local log file*, or to a UNIX-style *Syslog Server*.

An off-node server can aid in the management of a site with multiple systems, since all systems can send their log messages to a central log server. Note that in the case where multiple systems are logging their reports to a single Syslog Server, the system name is used to distinguish which system logged which report. This makes it crucial that each system be assigned a system name that is unique within its environment.

LOCAL LOG FILE OVERVIEW

The local log file is a circular file stored in RAM. It contains a fixed number of records. After the log is full, each new record overwrites the oldest record in the file.

Note: The CDR local log is intended for diagnostic use and is not suitable for production use as a CDR log.

SYSLOG SERVER OVERVIEW

When you specify an offnode Syslog Server as the destination for log reports, you have more direct control over:

- the allocation of disk space
- the integrity of disk space (redundant, tape backup, UPS, etc.)

- the ease of data retrieval
- the management of a multi-node site; all nodes can send their log messages to a central log server

Offnode log servers must be accessible via the system's LAN port; they cannot be accessed via the WAN. In addition, it is recommended that the log servers either be located on the same LAN segment as the system, or that a static route be defined for the log server. If a routing protocol such as RIP is used to establish a route to the log server, the server will be unavailable for the first 90 to 180 seconds after loading the system — until the route is established. This will cause log messages to be lost that are generated in the first 90 to 180 seconds of operation.

When we use the term UNIX Syslog Server, we are, more precisely, referring to the "syslogd" daemon running on a UNIX system. Syslogd reads and forwards messages to the appropriate log files and devices depending upon its configuration. Refer to your UNIX system documentation for more information on syslogd.

Each log message sent to a syslogd server has a priority tag associated with it. The priority tag is encoded as a combination: *facility*.*level*. The *facility* identifies the part of the system creating the log message and the *level* describes the severity of the condition which caused the log message to be written.

When sending a log message to a Syslog Server, the message is formatted as an ASCII string with the first item in the string being the syslog priority enclosed in angle brackets. The priority is presented as a decimal value, not a hexadecimal value. For example, to log the string "CDR VERIFY" with a priority of authentication.info, the priority (26 hex) would be converted to 38 decimal and the Syslog Server would be sent the string "<38> CDR VERIFY". The Syslog daemon will use the priority of 38 (26 hex) to determine where the message should be sent or stored. The string "CDR VERIFY" will then be sent to that destination.

The priority tag is implemented as an 8 bit hexadecimal integer. The low order three bits contain the severity level; the high order 5 bits contain the facility. Thus, for a convenient example, level info is encoded as the value 6 and facility authentication is encoded as the value 4 (in BSD UNIX v4.3). These two fields are combined as follows:

- level '6' => 06 hex
- facility '4' shifted left 3 bits to use the high order 5 bits => 20 hex
- bitwise OR the two values together => 26 hex

In result, priority of authentication.info is encoded as 26 hex.

Note: Because the values for both the facilities and the severity levels may vary from one version of UNIX to the next, the system allows you to set the entire priority value as an integer. This integer will be prepended to all messages sent to the Syslog Server.

One of the sources from which syslogd accepts log messages is UDP port 514. This is the access point that a subsystem uses when logging to a Syslog Server. The subsystem sends its log messages to UDP port 514 at the server's IP address.

Syslog Servers use UDP which is a datagram service. When a datagram is sent to a Syslog Server, there is no acknowledgment that the datagram was properly received. To reduce the possibility of lost data, two Syslog Servers may be used. The two resulting log files can be compared to detect missing data in one or the other.

SYSTEM MESSAGES

The CyberSWITCH reports three different types of system messages: informational, warning, and error messages. These messages are always available on-node via the `dr` command. To send system message reports to an off-node server, however, you will need to properly configure the setup. First, you must configure IP Routing, a LAN IP interface and an IP route to the log server. Then you must enable the *System Message (DR) log* feature:

- define and configure at least one log device for system messages
- connect the *Syslog Server* via the LAN port of the CyberSWITCH, and
- select an associated UNIX priority tag (default = 38)

Since multiple systems may log into a shared, central log server, it is crucial that each system Name be a unique value. This unique NAS (system) Name is used in the format of the message:

<NAS Name>: <Message Text>

An entire chapter is devoted to the listing and descriptions of the message text. Refer to the *System Messages* chapter for more information.

AUTHENTICATION MESSAGES

CyberSWITCH software now separates the authentication messages from other system messages and places them in their own log. Like the system messages, these authentication messages are always available on-node. You may access these messages via the `da` command. To send system message reports to an off-node server, however, you will need to properly configure the setup, similar to the procedure for System Messages: First, configure IP Routing, a LAN IP interface and an IP route to the log server. Next, enable the *Authentication Message (DA) log* feature:

- define and configure at least one log device for authentication messages
- connect the *Syslog Server* via the LAN port of the CyberSWITCH, and
- select an associated UNIX priority tag (default = 38)

Since multiple systems may log into a shared, central log server, it is crucial that each system Name be a unique value. This unique NAS (system) Name is used in the format of the message:

<NAS Name>: <Message Text>

An entire chapter is devoted to the listing and descriptions of the message text. Refer to the *System Messages* chapter for more information.

CALL DETAIL RECORDING

The CyberSWITCH's Call Detail Recording (CDR) feature tracks WAN connections on a per user or per device basis. This feature provides you with a way to account for usage of equipment and attached telephone lines.

CDR consists of a series of *reports* about an event, sent to either a local log file or an off-node database. For switched circuit devices, such as ISDN, the primary events are "connect", "disconnect" and "reject". For async terminal connections, they are "term conn", "term disc", "term succ" and "term fail". A report always refers to the particular entity at the other end of the WAN connection.

CDR is always active and available on-node via the `log cdr display` command. To send CDR reports to an off-node server, however, you will need to properly configure the setup. First, you

must configure IP Routing, a LAN IP interface and an IP route to the log server. Then you must enable the CDR feature:

- define and configure at least one log device for CDR
- connect the *Syslog Server* via the LAN port of the CyberSWITCH, and
- select an associated UNIX priority tag (default = 38)

CDR Log Report

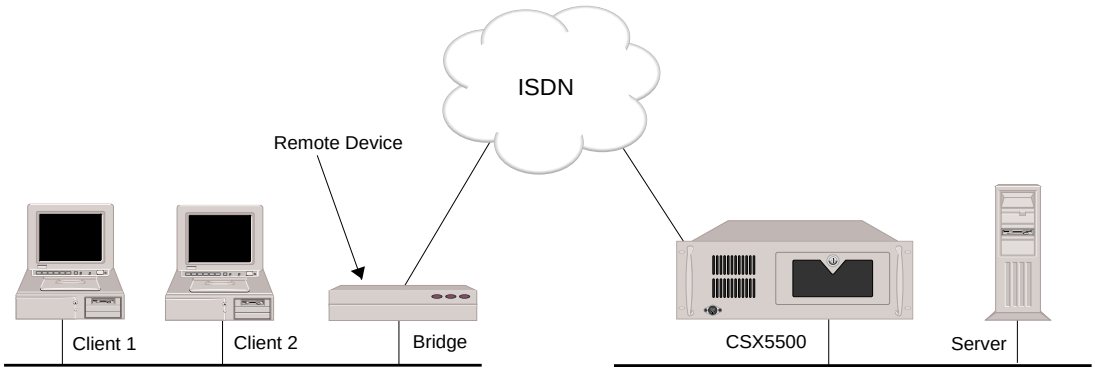
This option allows you to select the storage destination of your CDR log reports. You may send the CDR log reports to the local log, or to a previously configured offnode Syslog Server(s). A total of three destinations may be selected. For example, you could select the local log, and two previously configured Syslog Servers for your CDR log reports' destinations.

Storage on the local log is not recommended for production use; it is intended primarily for diagnostic use. This is because the local log only retains a fixed number of log entries. Once the file is full, each new entry overwrites the oldest entry. This will not give you a complete CDR Log.

CDR reports sent to the local file can be written to disk by issuing the `log cdr write` command. The file is then written to the \LOG directory. The file name is CDR_LOG. The file extensions are .1, .2, and so on up to .10. The file extension cycles through the values 1 through 10 with each write command, similar to the current report log file and status log file, so that the ten most recent versions of the CDR log are available on the system disk.

There are five ISDN CDR events that are logged: connect, disconnect, reject, system up, and verify. There are four Terminal Server events that are logged: Term Conn (connect), Term Disc (disconnect), Term Succ (successful authentication), and Term Fail (failed authentication). For each type of event that is logged, related CDR information is provided.

A report always refers to the particular device at the other end of the WAN connection. There is an important distinction between CDR on an interconnect device and CDR on a terminal server. The remote device for an interconnect device is the device on the other end of the WAN connection, not the human user or the client PC. For example, in the diagram below, it is Bridge that is the system's remote device, not Client1 (the machine) or Client2, and not the user, who is using Client1.



A CDR report contains a variety of data items related to an associated CDR event. Some reports consist of more than one record.

Call Detail Recording Events

For switched ISDN services:
There are five ISDN CDR events: connect, disconnect, reject, system up, and verify.

A connect event occurs when the system authenticates the remote device of an ISDN connection. The time stamp for the connect event marks the time the ISDN connection was established.

A disconnect event occurs when the system disconnects a connected device. The disconnect timestamp marks the time that the decision to disconnect was made.

A reject event occurs when the system disconnects an ISDN connection for which no device was authenticated. The reject timestamp marks the time that the decision to disconnect was made.

A system up event occurs when the system is loaded. The system up event provides a visible divider in the log file between two instances of loading the system. Since the connection ID value is a counter that begins at zero when the system is loaded, it is necessary that the log file contain an indication of when the system is loaded.

A verify event is generated by issuing the `cdr verify` console command. This command verifies the configuration of the CDR feature. It causes a message to be sent to all configured CDR log servers. The proper logging of the message can then be inspected to verify that CDR configuration is as desired.

For Terminal Servers:
There are four terminal server events: Term Conn, Term Disc, Term Succ, Term Fail.

A Term Conn event occurs when the system identifies a call as an asynchronous terminal connection. The time stamp marks the time when this connection is identified, not when the call is actually received. Modem negotiation takes place before the time stamp and protocol identification (async terminal vs. PPP).

A Term Disc event occurs when a terminal connection disconnects prior to switching to PPP mode. This can occur as a result of a modem call disconnecting, a user level authentication failure, or a logout (in the case of terminals used to access the admin login prompt).

A term Succ event occurs when a terminal connection passes user level authentication.

A Term Fail event occurs when a terminal connection fails user level authentication.

Event Report Contents

A CDR event triggers a report which can consist of one or more records. Each record corresponds to a line in the log file. This alleviates any constraints of having to fit a report in an 80 character string. Reports are sent to some sort of log device; either a local log file or an offnode Syslog Server.

Each ISDN connection is assigned a connection Id to uniquely identify the connection on its system. This connection Id is presented on CDR reports so that all the records of a CDR report have the same connection Id and can be associated, thereby the Connect and Disconnect reports for a given connection can be associated by their matching connection Id field.

When multiple systems are logging to a shared, central log server, the combination of NAS name, Event and Connection Id allows all the records of a report to be processed without ambiguity. (It is crucial, in this case, that each system Name be set to a unique value; otherwise, it will be impossible to distinguish the NAS which originated a CDR report).

A multi-channel connection is reported as a set of discrete connections to the same device (that happen to coincide).

The record format of all CDR reports is consistent, so that all reports have a first record with identical fields, all reports which have a second record, have identical fields in this record, etc.

The record formats for the four types of records available for event reports are as follows:

Record 1
```
<NAS Name>< ConnectionId>< Event Type>< 1 OF n>< Remote Device Name>< PORT s/l/b>
```

Record 2
```
<NAS Name><ConnectionId><Event Type>< 2 OF n>< Direction><phone number if available>
```

Record 3
```
<NAS Name><ConnectionId><Event Type>< 3 OF n><Data Rate><Timestamp>
```

Record 4
```
<NAS Name><ConnectionId><Event Type><4 OF n><Duration>
```

The following fields are defined for the CDR Event Reports. The precise meaning of some fields, timestamp for example, will vary depending upon which report the field is in. These variations are defined further when the report contents are described.

CALLING DIRECTION
This indicates which side initiated the connection. Possible values are “IN FROM” and “OUT TO”.

CONNECT TIME
Refer to “Duration”.

CONNECTION ID
This field is used to correlate all records involving a particular ISDN connection. The field is an unsigned long hexadecimal integer. It begins at zero when the system is loaded and increments by one to 0FFFFFFFF hex, at which point it wraps back to zero. This provides for somewhat over four billion connections before a connection Id is re-used.

DATA RATE
This field indicates the data rate for a B channel. The possible values are 56 Kb, 64 Kb and 384 Kb. Note: The data rate for modem connections is currently reported as the ISDN rate of the consumed channel (i.e., 56KB or 64KB).

DURATION
This field reflects the time that a connection is active; it is presented in hours, minutes and seconds. The precise meaning varies somewhat for a successful connection versus a call rejection.

EVENT TYPE
This field indicates what type of event the associated message is reporting. The possible values are 'CONNECT', 'DISCONNECT', 'REJECT','TERM CONN','TERM DISC','TERM SUCC','TERM FAIL', 'SYSTEM UP' and 'CDR VERIFY'.

NAS NAME
NAS Name (Network Access Server Name) contains the System Name of the system logging the message.

PHONE NUMBER
On incoming calls this field contains the Calling Line Id of the caller if the information is available (some switches do not provide Calling Line Id). On outgoing calls, this field contains the phone number of the remote device that the system is calling.

REMOTE DEVICE NAME
This field contains the name of the remote device, if available.

SLOT, LINE AND BEARER
This field identifies the slot (or resource), the line and the bearer channel used for the associated connection.

TIME STAMP
The field contains the time and date. The meaning of this field varies depending upon the report.

Connect/Term Connect Event Report Contents

On a connect event, records 1 through 3 are used. The event type is CONNECT or TERM CONN. The time stamp reflects the time that the ISDN connect message was received from the switch. An incoming phone number is displayed if it is provided by the telephone switch. Not all switches provide calling line identification. A phone number is always displayed for outbound calls.

example 1:

```
Chicago-Schaumburg 00000001 CONNECT 1 OF 3 MonroeCounty PORT 1/1/1
Chicago-Schaumburg 00000001 CONNECT 2 OF 3 IN FROM 3135551212
Chicago-Schaumburg 00000001 CONNECT 3 OF 3 64Kb 08/28/97 23:11:55
```

example 2:

```
Chicago-Schaumburg 00000001 CONNECT 1 OF 3 MonroeCounty PORT 1/1/1
Chicago-Schaumburg 00000001 CONNECT 2 OF 3 OUT TO 3135551212
Chicago-Schaumburg 00000001 CONNECT 3 OF 3 64Kb 08/28/97 23:11:55
```

Note: In most cases, a device is identified when a connect event occurs and the device name is included in the connect report. With user level security, the connect event occurs before the user is identified. Therefore, the connect report will contain a name of UNKNOWN. The disconnect report will have the actual user name, as determined by SENTRY. The connection Id from the connect and disconnect reports will match.

Disconnect/Term Disconnect Event Report Contents

On a disconnect event, records 1 through 4 are used. The event type is DISCONNECT or TERM DISC. The time stamp reflects the time that the decision to disconnect was made. The phone number displayed is the phone number that was used to dial out, or the incoming calling line id (depending on call direction).

The duration is calculated by subtracting the connect event time from the disconnect time.

Example:

```
Chicago-Schaumburg 00000001 DISCONNECT 1 OF 4 MonroeCounty PORT 1/1/1
Chicago-Schaumburg 00000001 DISCONNECT 2 OF 4 IN FROM 3135551212
Chicago-Schaumburg 00000001 DISCONNECT 3 OF 4 64Kb 08/28/97 23:11:55
Chicago-Schaumburg 00000001 DISCONNECT 4 OF 4 DURATION 01:11:55
```

Reject Event Report Contents

On a reject event, records 1 through 4 are used. The event type is REJECT. The timestamp reflects the time that the decision to disconnect was made. An incoming phone number is displayed if it is provided by the telephone switch. Not all switches provide calling line identification. A phone number is always displayed for outbound calls.

The duration is calculated by subtracting the ISDN connection timestamp (the time that the ISDN connect message was received from the switch) from the reject event timestamp.

Example:

```
Chicago-Schaumburg 00000001 REJECT 1 OF 4 UNKNOWN PORT 1/1/1
Chicago-Schaumburg 00000001 REJECT 2 OF 4 IN FROM 3135551212
Chicago-Schaumburg 00000001 REJECT 3 OF 4 64Kb 08/28/97 23:11:55
Chicago-Schaumburg 00000001 REJECT 4 OF 4 DURATION 00:00:07
```

Term Succ Event Report Contents

On a Term Succ event, records 1 through 3 are used. The event type is TERM SUCC. The time stamp represents the time at which the user level authentication succeeded. The port, call direction and phone number information are the same as for a Term Conn event.

Example:

```
Chicago-Schaumburg 00000001 TERM SUCC 1 OF 3 UNKNOWN PORT 1/1/1
Chicago-Schaumburg 00000001 TERM SUCC 2 OF 3 IN FROM 3135551212
Chicago-Schaumburg 00000001 TERM SUCC 3 OF 3 64Kb 06/16/98 23:11:55
```

Term Fail Event Report Contents

On a Term Fail event, records 1 through 3 are used. The event type is TERM FAIL. The time stamp represents the time at which the user authentication failed. The PORT, call direction and phone number information are the same as for a Term Conn event.

Example:

```
Chicago-Schaumburg 00000001 TERM FAIL 1 OF 3 UNKNOWN PORT 1/1/1
Chicago-Schaumburg 00000001 TERM FAIL 2 OF 3 IN FROM 3135551212
Chicago-Schaumburg 00000001 TERM FAIL 3 OF 3 64Kb 06/16/98 23:11:55
```

System Up Event Report Contents

On a System Up event, only record 1 is used. The event type is SYSTEM UP. No data is filled in for the Remote Device Name field or the Port field.

Example:

```
Chicago-Schaumburg SYSTEM UP 1 OF 1
```

Verify Event Report Contents

On a Verify event, only record 1 is used. The event type is CDR VERIFY. No data is filled in for the Remote Device Name field or the Port field.

Example:

```
Chicago-Schaumburg CDR VERIFY 1 OF 1
```

COMPRESSION OPTIONS

Compression allows the CyberSWITCH to compress outgoing data and decompress incoming data. This allows user devices on the WAN to initiate a connection to the system over the switched digital network and transmit and receive compressed data, thereby increasing the amount of data that can be transmitted over the line and decreasing the transmission time.

CONFIGURING COMPRESSION OPTIONS

USING CFGEDIT

1. Select *Compression Options* from the options menu. The following menu will be displayed:

```
Compression Options Menu:

   1) Compression Subsystem (Enable/Disable)
   2) Default Per-Device Compression setting (Enable/Disable)
   3) Starting PPP STAC-LZS Sequence Number

Select function from above or <RET> for previous menu:
```

2. Select option 1 and follow the onscreen instructions to enable compression on a system-wide basis. If enabled, the system will negotiate compression with remote devices per their individual device configuration. If disabled, the system will not negotiate compression with any remote device.

3. Select option 2 and follow the onscreen instructions to either enable or disable per-device compression. This defines the initial value for the per-device state when a new device is added to the on-node device table. Or, if the device is authenticated via an off node server, the device will be given its compression enable / disable state based on this value when no value is delivered by the off-node database.

4. Option 3 is only applicable when using PPP compression with the STAC-LZS protocol. This allows you to change the starting PPP STAC-LZS sequence number for devices that do not have the starting sequence of 1.

COMPRESSION OPTIONS CONFIGURATION ELEMENTS

COMPRESSION SUBSYSTEM STATUS

You may enable or disable the compression subsystem status. This option provides enable / disable control over the entire compression subsystem within the system. If this option is enabled, the system will negotiate compression with remote devices per their individual *device compression configuration*. If this option is disabled, the system will not negotiate compression with any remote device. The default value is enabled.

Note that enable / disable applies to *all* protocols which support compression.

DEFAULT PER-DEVICE COMPRESSION SETTING

You may enable or disable the per-device compression setting. This is in addition to the global compression enable / disable state described above. The Default Per-Device Compression setting defines the initial value for the per-device state when you add a new device to the on-node device table. Or, if the device is authenticated via an off node server, the device will be given its compression enable / disable state based on this value when no value is delivered by the off-node database.

You may later change a specific device's enable / disable state.

The per-device compression enable / disable state is only supported for connections using the PPP protocol. The default value is enabled.

STARTING PPP STAC-LZS SEQUENCE NUMBER

Default value is 1. When using PPP Compression with the STAC-LZS protocol, a sequence numbering scheme can be used whose initial value is required to be 1 by the protocol specification. Some devices from other vendors do not start with 1. This results in a resynchronization sequence on the first frame which is exchanged. When the user device fully supports the CCP protocol's Reset mechanism, this will only result in the minor inconvenience of a lost frame at the beginning of a session. However, if such a device's resynchronization mechanism is to completely renegotiate CCP, this sequence will repeat infinitely.

This option provides an escape mechanism to allow interworking with such devices by modifying the initial PPP STAC sequence number.

The Starting PPP STAC Sequence Number is maintained for each device. The value which appears on this configuration screen provides the default value for the per-device value. When you add a new device to the on-node device table, that device's starting sequence number option will be assigned the value which appears on this screen. You can then change this for each individual device. Or, if the device is authenticated via an off node server that does not deliver a value for this configuration item, the device will be given its starting sequence number from the value on this menu

As its name implies, this option only applies to connections which utilize the PPP protocol with STAC-LZS compression and sequence numbers checking.

COMPRESSION OPTIONS BACKGROUND INFORMATION

The system data compression capability allows the system to negotiate compression algorithms with a remote device. This compression can be done using some proprietary bridging protocols and also the PPP CCP protocol.

After successfully negotiating compression, data is compressed by a peer and transmitted to the system. The system decompresses the data, processes the addressing information contained in the device data, and transmits the data as required. The converse is also true, the system can receive data coming from a WAN or LAN, compresses the data before transmitting it to a peer. The net effect is to increase effective interconnect bandwidth by decreasing transmission time. If negotiation for compression fails, data is transmitted uncompressed.

The compression algorithm implemented is STAC-LZS. This algorithm is used in all of STAC's data compression products. This software version is fully compatible with STAC's data compression compressor chips including the multi-tasking features. STAC-LZS data compression is performed by replacing redundant strings in a data stream with shorter tokens. The STAC-LZS uses a compression history, or sliding window, as opposed to a structured dictionary. This allows greater flexibility and a greater number of possible string comparisons during compression process. The compression history automatically discards old information as new information is processed. Both the device and system must perform compression using the STAC-LZS data compression algorithm. The peer and remote compression algorithms must be synchronized, this is accomplished by negotiating compression at channel connect time. Once this has been accomplished compressed data can be transmitted. If a transmission problem should ever occur the problem is detected and compression re-synchronized by the execution of a pre-defined protocol.

COMPRESSION AND CCP

The Compression Control Protocol (CCP) is one of a suite of protocols which operate under the umbrella of the IETF's Point-to-Point Protocol (PPP) suite. CCP implementation permits compression and decompression on PPP links.

During call establishment, an appropriately configured system will attempt to negotiate compression using CCP and STAC-LZS. The system will support either of two STAC-LZS modes, sequence numbers or extended mode. This negotiation will take place on all calls. Specific options used by CCP include:

- STAC-LZS compression algorithm
- one history
- sequence number check mode or extended mode

During CCP negotiations, the system will always propose the use of Sequence Number check mode first for inbound traffic. The peer has the option to accept or reject this proposal. If the peer rejects the proposal and counter-proposes STAC-LZS Extended mode, it will be accepted by the system. For outbound traffic, the system will accept either Sequence Number or Extended Mode.

Once compression has been negotiated, transfers of compressed data can take place across the Point-to-Point links. Such compressed data packets will be encapsulated as described in the CCP specification. Received data packets not so encapsulated will be considered to be uncompressed data and will be forwarded on in the order they were received. Transmitted packets whose compressed size increases to the point of exceeding the link's Maximum Receive Unit (MRU) will be sent uncompressed.

When using Sequence Number check mode and a non-zero number of histories, the STAC-LZS algorithm requires that incoming data packets be decompressed in the order they were compressed. The sequence numbers are used to assure proper ordering and that no packets have been lost. Should a packet loss be detected, the system will send a CCP Reset-Request packet as described in the CCP specification to the peer and will discard any accumulated history and queued receive packets. The peer will be expected to also discard its outbound history and respond with a CCP Reset-Acknowledgment. At this point, both sides will have been resynchronized and compressed data transfers can continue.

When using Extended mode, a coherency count is checked to detect lost packets. If a packet loss is detected by the receiver, a Reset-Request is sent to the transmitter. The next compressed data packet transmitted will have a bit set to indicate that the history has been reset.

With the use of sequence numbers, the decompressed output of all in-order compressed frames is assumed to be valid. The correct CRC check of the underlying link, combined with the in-order sequencing of the frames, is the basis for assuming that the data yielded by the decompression is accurate. However, even when these conditions have been met, the internal STAC library can still signal a decompression failure. This type of error in the peer device is not considered to be recoverable, as it indicates a flawed compressed packet from the decompressing system's point of view. Therefore, should such an error occur, CCP will be closed and the connection will continue to operate, albeit without compression. An error message will be logged indicating an internal decompression failure.

Compression is negotiated independently on inbound and outbound channels. It is possible to provide compression in one direction while not in the opposite direction.

Should the peer not support PPP compression, CCP will fail to converge and the link will continue to operate without providing compression. Should the peer support CCP, but not the Stac protocol, the CCP negotiation will succeed, but no actual compression will occur on the connection.

Note: The CyberSWITCH does not support individual link compression when PPP Multilink is negotiated to aggregate multiple links. Multiple links to a single destination will be treated as a single high capacity link as far as PPP compression is concerned. One history will be kept for the group of links, and packets will be compressed before they are fragmented for transmission across the multiple links.

The following documents provide additional information about PPP Compression:

- The PPP Compression Control Protocol (CCP); RFC 1962; Dave Rand; June, 1996.
- PPP Stac LZS Compression Protocol; RFC 1974; Robert Friend and William Allen Simpson; August 1996.

TFTP

CONFIGURING TFTP

Note: You cannot configure TFTP through CFGEDIT. The configuration can only be done through Manage Mode commands.

USING MANAGE MODE COMMANDS

tftp

This command displays the current TFTP configuration. The TFTP configuration information includes the following items:

- operational status of the TFTP feature (enabled or disabled)
- operational status of the TFTP Client (enabled or disabled)
- operational status of the TFTP Server (enabled or disabled)
- the file access rights for the TFTP Server (ADMIN or GUEST)

tftp change

This command allows you to change the current TFTP configuration. You can enable or disable the TFTP feature, TFTP Client, and the TFTP Server. You can also change the file access rights for the TFTP Server.

TFTP CONFIGURATION ELEMENTS

OPERATIONAL STATUS OF TFTP FEATURE
You can enable or disable the TFTP feature.

OPERATIONAL STATUS OF TFTP CLIENT
You can enable or disable the TFTP client feature. The TFTP client functions are achieved through administration console commands.

OPERATIONAL STATUS OF TFTP SERVER
You can enable or disable the TFTP server feature. The TFTP Server function is invoked remotely from a TFTP host device connected to either a LAN or WAN network interface.

FILE ACCESS RIGHTS FOR THE TFTP SERVER
The file access rights associated with the configured device Id that are applied to all file accesses by the remote host.

TFTP BACKGROUND INFORMATION

The TFTP (Trivial File Transfer Protocol) feature provides the ability through the TFTP Server, to upload and download configuration, report, statistics, and other system files to or from a remote system. The TFTP feature also provides the capability from the console for the device to send and receive the same file types through the TFTP Client function.

The TFTP feature will provide controlled read (download) and write (upload) access by remote systems to configuration, report, statistics, and other system files on target systems through the TFTP Server. The system will also have the ability to upload and download these file types to or from target remote systems through a console invoked TFTP Client function.

Access to files on an system will be controlled by configuration through Manage Mode. File access attributes are associated with the existing system device id's (GUEST and ADMIN) to allow configuration of file access rights.

Configuration of the TFTP feature through Manage Mode allows the administrator to restrict upload and download access for each particular file type. The administrator can also disable the entire feature or a portion of the feature through Manage Mode.

The system provides both a TFTP client and a TFTP Server function. The TFTP Client is invoked via system commands from an administration session on the system console. The TFTP client uses the file access attributes of the currently logged in device id, either GUEST or ADMIN.

The TFTP Server function is invoked remotely from a TFTP host device connected to either a LAN or WAN network interface. The administrator sets the file access attributes for the TFTP Server function by associating an system device ID (GUEST or ADMIN) with the TFTP Server function. Whenever a remote host invokes the TFTP Server function in the system, the file access rights associated with the configured device ID are applied to all file accesses by the remote host.

Each device has pre-assigned configurable access rights to the TFTP permissible file types. The access rights are configurable using the ***`fileattr change`*** Manage Mode command. Refer to *File Attributes* for more information regarding configuring the file attributes.

When a device remotely access the TFTP server, it doesn't matter what level the device is logged in as. What matters is the device level that is configured for the Server on the system that is being logged into. It is this file access level (or device login level) that controls all remote devices accesses.

FILE ATTRIBUTES

CONFIGURING FILE ATTRIBUTES

Note: You cannot configure file attributes through CFGEDIT. The configuration can only be done through Manage Mode commands.

USING MANAGE MODE COMMANDS

`fileattr`

This command displays the current access rights for each access level depending on file types.

`fileattr change`

This command allows you to change the access rights for each access level, depending on file types.

FILE ATTRIBUTES CONFIGURATION ELEMENTS

FILE ATTRIBUTE

The access right for each access level assigned to each file type. Access rights include:

- read only access (R)
- write only access (W)
- read and write access (RW)
- no access rights (N)

FILE ATTRIBUTES BACKGROUND INFORMATION

The *tftp change* Manage Mode command allows you to assign the file access rights for the TFTP server (see *TFTP*). Using the *fileattr change* Manage Mode command, you can change the access rights for each access level, depending on file type.

The default file access for the GUEST device is "read" access to all files. The default file access for the ADMIN device is "read" access to the report and statistics files, with "read and write" access to all other files. The default for the TFTP server is ADMIN file access rights. The possible file types and possible accesses for each device are:

Users	*Report Files*	*StatFiles*	*CfgFiles*	*Other Files*
GUEST	RN	RN	RN	N
ADMIN	RN	RN	RWN	RWN

where:
- "R" is for read only file access
- "W" is for write only file access
- "RW" is for read and write access
- "N" is for no access rights for the corresponding file type

The file types that fall under the headings shown above are as follows:

File category	*File types included in the category*
REPORT	RPRT_LOG.1 - 10
STATISTICS	STAT_LOG.1 - 10
CONFIGURATION	*.NEI (with the exception of CFGTOKEN.NEI)
OTHERS	All other file types i.e. .EXE, .COM, .TXT, (CFGTOKEN.NEI), etc.

VERIFICATION AND DIAGNOSIS

After configuring your CyberSWITCH and before proceeding with normal system operations, we suggest you verify that the system is functional. This segment of the *User's Guide* provides instructions for verifying system hardware and system configuration, and then diagnosing potential problems encountered during the verification process.

We include the following chapters in this segment:

- *Verifying the Base System*
  Hardware resources, LAN and WAN connections, bridge and/or router initialization, alternate accesses, remote device connectivity, and security

- *Verifying Routing Protocols*
  IP, IPX, AppleTalk

- *Verifying System Options*
  SNMP, dial out, compression, reserved bandwidth, DHCP, semipermanent connections, proxy ARP

You only need to perform the verification procedures for the protocols and/or options that apply to your configuration. For example, if your configuration does not use SNMP, skip the SNMP verification section in the *Verifying System Options* chapter.

To perform the verification procedures, WAN lines must be available and ready to use. LAN attachment components must also be available and ready to use.

During some of the procedures, we ask you to enter an administration console command. To enter these commands, you must have an active administration session. If you need instructions for starting an administration session, refer to *Accessing the CyberSWITCH Accessing the CyberSWITCH.*

Also refer to the *Troubleshooting* segment for a complete listing of all system and trace messages, as well as system indicator descriptions.

VERIFYING THE BASE SYSTEM

OVERVIEW

This chapter describes the verification process for the base system. It includes the verification process for:

- *hardware resources*
- *WAN lines*
- *LAN connections*
- *bridge initialization*
- *routing initialization*
- *remote device connectivity*
- *multi-level security*
- *IP Host Mode*
- *alternate accesses*

To perform the verification procedures, WAN lines must be available and ready to use. LAN attachment components must also be available and ready to use.

During some of the procedures, we ask you to enter an administration console command. To enter these commands, you must have an active administration session. If you need instructions for starting an administration session, refer to *Accessing the CyberSWITCH*.

Note: At least one remote device is required to proceed with many of the verification procedures.

HARDWARE RESOURCES OPERATIONAL?

WAN ADAPTER INITIALIZED?

1. At the system prompt, enter the *dr* command to display current system messages. At the administration console type:

   dr <return>

2. For each WAN adapter installed, look for these WAN adapter initialization messages among the system messages:

   ```
   Bootstrap loaded on WAN card in slot <slot #>, waiting for response
   Bootstrap came alive on WAN card in slot <slot #>
   Downloading WAN card in slot <slot #> with operational software
   Waiting for WAN card in slot <slot #> to complete initialization
   WAN card in slot <slot #> signals it is operational
   ```

   If you see these WAN adapter initialization messages, then the WAN adapter in the indicated slot is operational. You may continue with the verification of the LAN adapter.

3. If these WAN adapter initialization messages are NOT displayed, and you see one of the following error messages, you may have a problem:

```
Error mapping WAN adapter # into Host memory map
Type mismatch of configured & installed adapter #
Error initializing WAN card: #
Failure during static RAM test on adapter #
Error downloading operational software to adapter #
Error downloading bootstrap program to adapter #
```

To correct the problem, try the following:

a. Verify the resource type and adapter configuration settings as described in the *Hardware Installation* chapter.

b. Check the configuration for the WAN Adapter resource. The configuration must match the resource and its given slot number. Refer to the *Configuring Resources and Lines* chapter.

c. If these actions fail to correct this problem, check to see if the WAN adapter is properly installed in the CyberSWITCH. Refer to the *Hardware Installation* chapter.

CAUTION:
If at any time you need to remove the system cover, be sure to turn the system OFF and unplug it first.

Note: A Robbed Bit Signaling line will display a “Layer 1 up” message, but since an RBS resource does not have an ISDN layer two, a “Data link up” message will not be displayed.

LAN ADAPTER INITIALIZED?

1. Determine if the LAN adapter resource is operational by viewing the system messages. At the administration console type:
   dr <return>

   The *dr* command displays the current system messages. Look for these LAN adapter initialization messages among the system messages:

   ```
   LAN Adapter Reset
   LAN Adapter ROM version #.#.#
   ```

   Note: Other messages may also be displayed with the LAN adapter initialization messages.

2. If these LAN adapter initialization messages are NOT displayed, and you see one of the following error messages, you may have a problem:

   ```
   Invalid LAN Adapter identifier
   LAN Adapter Command Timeout
   LAN Adapter FIFO not empty, status = #
   LAN Adapter LAN Controller error
   LAN Adapter Response Timeout
   MAC layer Bridge did not Initialize
   [IP] Initialization failure
   ```

To correct the problem, try the following:

a. Verify the resource type and adapter configuration settings as described in the *Hardware Overview* and *Hardware Installation* chapter.

b. Check the configuration for the LAN Adapter resource. The configuration must match the resource and its given slot number. Refer to the *Configuring Resources and Lines* chapter.

c. If actions *a* or *b* fail to correct this problem, check to see if the LAN adapter is properly installed in the CyberSWITCH. Refer to the *Hardware Installation* chapter.

d. If actions *a*, *b*, or *c* fail to correct this problem, the LAN adapter may be faulty. If you have a spare LAN adapter resource available, replace the faulty LAN adapter with the spare. Contact Customer Support.

CAUTION:
If at any time you need to remove the system cover, be sure to turn the system OFF and unplug it first.

WAN LINES AVAILABLE FOR USE?

VERIFYING WAN LINE AVAILABILITY

1. Determine if WAN lines are operational by viewing the system messages. At the administration console type:
   dr <return>

2. For each basic rate or primary rate line configured and attached to the CyberSWITCH, the following line initialization message should be displayed among the system messages:
   `Data Link up: <slot #> <port #> <ces>`

   If this message is displayed for each configured line, then the WAN lines are available for use.

   Notes: Depending on the resource switch type, the system will delay up to 2 minutes before attempting to bring up the data links.

   Other messages may also be displayed with the line initialization messages.

3. If the WAN lines are NOT available, the system may display one of the following messages on the LCD:
   ```
   Line (slot #, port #) down
   Out Svc 1 (slot #, port #)
   Out Svc (2, 3, 4, or 5) (slot #, port #)
   ```

   To correct the problem, try the following:

   `Line (slot #, port #) down:`
   a. Verify that the line is correctly attached to the proper system resource and port.
   b. If the line was correctly attached, try restarting the system.

   `Out Svc 1 (slot #, port)?`
   (Layer 1 cannot be established, most likely due to WAN cabling problems.)

a. If the system has been operational for longer than 2 minutes, verify that the line is correctly attached to the proper system resource and port. If not, wait for 2 minutes and check again for the WAN line availability messages.
b. If using a NT1 or CSU, examine the local and network lights of the NT1 or CSU. If the local light is on, try another cable between the CyberSWITCH and the NT1 or CSU. If the local light is not on, but the network error light is on, contact your line provider.
c. If the line was correctly attached, turn the system off, then on. If this fails to correct the problem, continue with the next step.
d. If using PRI, refer to the *Basic Information for Ordering PRI ISDN Lines* section found in the *Ordering ISDN Service* chapter. Compare the parameters with those required by the PRI line provider. It is possible that there is a mismatch.

`Out Svc (2, 3, 4, or 5) (slot #, port #)`
(Layer 2 cannot be established, most likely due to an invalid configuration.)
a. If the system has been operational for longer than 2 minutes, verify that the line is correctly attached to the proper system resource and port. If not, wait for 2 minutes and check again for the WAN line availability messages.
b. If the line was correctly attached, turn the system off, then on. If this fails to correct the problem, continue with the next step.
c. For the "Out Svc2 (slot #, port #)" message with a Basic Rate line, check configuration. "Auto TEI" should be selected. Reconfigure if necessary.
d. For the "Out Svc2 (slot #, port #)" message with a Primary Rate line, call your line provider and have the data link restarted.
e. For the "Out Svc3 (slot #, port #)" on an Auto TEI line, check configuration. Try reconfiguring the line using non-auto TEI.

4. If a WAN line is still unavailable, issue the *dr* console command. If these two messages are displayed together, you may have a data link problem:

```
WAN card in slot <slot #> signals it is operational
Abnormal response rcvd: state=-1 msg=73 reason=6 cc state=-1
```

To correct the problem, try the following:

Check the configuration. Verify that all lines are configured with corresponding data links. If this is not the case, add data links to all configured lines.

5. If the above actions fail to correct problems, then call your phone company (carrier) to check the status of the line. If it is determined that there is no problem with the line, contact Customer Support.

DEDICATED SERIAL CONNECTIONS

1. View the system messages for information on dedicated serial connections. At the administration console type:
   dr <return>

2. The following messages may indicate a problem:

```
Error mapping adapter # into Host memory map
Type mismatch of configured & installed adapter #
Serial dedicated down: Slot #, Port #
```

3. *To correct the problem, try the following:*

```
Error mapping adapter # into Host memory map
Type mismatch of configured & installed adapter #
```

a. Terminate the system software:
Type: *quit*<return>

Check the configuration for the Serial Adapter resource. The configuration must match the resource type and hardware settings. For details, refer to the *Hardware Overview* and the *Hardware Installation* chapter.

Turn the CyberSWITCH off, then on
Press: <Power Off><Power On>

Continue with step 1 in the section *Verifying WAN Line Availability* (and reestablish the administration session, if necessary).

b. If this fails to correct this problem, check to see if the Serial adapter is properly installed in the system.

```
Serial dedicated down: Slot #, Port #
```

a. Check that the serial cable is properly connected to the Serial Adapter resource.

Continue with step 1 in the section *Verifying WAN Line Availability* (and reestablish the administration session, if necessary).

b. If this fails to correct this problem, check to see that the Serial cable is properly connected to the network termination equipment.

c. If the above actions fail to correct this problem, check that the serial adapter is configured to match the network requirements.

4. If this fails to correct the problem, the Serial adapter may be faulty. If you have a spare Serial adapter resource available, replace the faulty Serial adapter with the spare. Contact Customer Support.

CAUTION:
If at any time you need to remove the system cover, be sure to turn the system OFF and unplug it first.

LAN Connection Operational?

To verify the operation of the LAN connection, the Ethernet LAN adapter resource must already be operational:

1. Connect the CyberSWITCH to a properly terminated Ethernet LAN. Note that an external MAU (and AUI cable if needed) is required for this connection.

2. Transmit a test packet onto the Ethernet LAN. At the administration console type:
lan test <return>

This command will display a message similar to the following:

```
LAN port 1 Transmit was successful
```

If the system displays this message, then the test packet was transmitted correctly.

3. If you receive the message:

```
LAN port 1 Transmit was not successful
```

Try the following to correct the problem:

a. Check to see if the Ethernet LAN is properly connected to the CyberSWITCH.
b. Check to see if the Ethernet LAN is properly terminated.
(Test: Can any other machine transmit data successfully onto this LAN?)
c. If the problem is still not resolved, contact Customer Support.

BRIDGE INITIALIZED?

1. Determine if the bridge is in the forwarding state by viewing the system messages. At the administration console type:

dr <return>

2. The *dr* command displays the current system messages. Look for the following LAN adapter messages among the system messages:

```
LAN Port <port #> is now in the LISTENING state
LAN Port <port #> is now in the LEARNING state
LAN Port <port #> is now in the FORWARDING state
```

Note: Other messages may also be displayed with these LAN messages.

If you see these bridge initialization messages, then bridging is operational.

3. If these messages are NOT displayed, try the following:
a. Make sure the *LAN Adapter* has initialized correctly.
b. Check the configuration to verify the bridge is enabled.

IP ROUTER INITIALIZED?

1. View the system messages. At the administration console type:

dr <return>

2. Look for the following IP message among the system messages:

```
[IP] IP router is initialized successfully
```

3. For each IP interface that has been configured, the following interface initialization message should be displayed among the system messages.

```
[IP] Network initialized successfully on ddd.ddd.ddd.ddd
```

Note: Other messages may also be displayed with the IP router initialization messages.

If you see these IP router initialization messages, then the IP router is operational.

4. If you do NOT see the initialization message, check the configuration to verify that IP routing is enabled.

5. If IP routing is enabled, and you still do NOT receive a successful initialization message, it may be that you have either not configured a needed interface or have incorrectly configured an interface. Check the system's IP network interface configuration using the *ipnetif* command (a Manage Mode command). If there is a problem with the configuration, use *CFGEDIT* to make corrections.

REMOTE DEVICE CONNECTIVITY

To verify remote device connectivity to the CyberSWITCH, the WAN lines that are connected to the system must be available for use, and the bridging and/or routing options must be properly initialized. The remote devices must be operational and available to initiate ISDN WAN connections.

The method of connection initiation is dependent upon the remote device type. Refer to the remote device documentation to determine how to initiate an ISDN WAN connection.

To verify connectivity:

1. In a controlled manner, initiate an ISDN connection from each remote device.

2. When each remote device connects to the system, it will appear as either a "REMOTE site" or as the configured Device Name (if security is enabled) on the Monitor Connections screen. To display the Monitor Connections screen, enter the following console command:

   mc <return>

   Note: The terminal type must be the same for Telnet and the terminal emulation. Use the *term set* administration console command to set the terminal type.

   If each remote device is able to connect to the CyberSWITCH, then WAN connectivity is successful.

3. If the remote device is NOT able to connect to the CyberSWITCH, try the following:

   a. Set-up:

   The system software should be up and running. (At the administration console: if you are in the Connection Monitor window, exit to the "[System Name] >" prompt.)

   - Enable the call trace messages with the *trace on* console command.
   - Erase the current system messages using the *er* console command.
   - In a controlled manner, initiate an ISDN connection from the remote device.

   b. Action:

   - After a connection has been initiated, view the system messages (by issuing the *dr* console command). Look for the following call request messages among the system messages:

```
In - INCOMING CALL Call Id=<call Id> Slot =<slot #> Port=<port
#> Chans=<bearer channel map> Ces=<comm endpoint suffix>
Rate=<data rate>
Out - CONNECT Call Id=<call Id> Slot=<slot #> Port=<port #>
Chans=<bearer channel map> Ces=<communication endpoint suf-
```

```
fix> ConnId=<connect Id>
In - CONNECT Call Id=<call Id> Slot=<slot#> Port=<port #>
Chans=<bearer channel map> Ces=<communication endpoint suf-
fix> ConnId=<connect Id>
```

If the system reports these messages, then continue with the next step.

If the system does NOT report these messages, the remote device is not correctly connecting to the system. Check and verify the configuration of the remote device.

4. If the system displays the following message among the system messages:
   `Security Rejection-Invalid Calling Line Id - <#>`

   the network is indicating a calling line identifier that is not configured for any valid device in the system Device list. The number "#" indicates the actual number presented by the network.

5. For Remote Bridge Devices:
   If the system displays the following messages among the system messages:
   ```
   Security Rejection - Caller did not negotiate security
   Security Rejection - No Bridge Address given by caller
   Security Rejection - Unknown Calling Bridge
   Security Rejection - No Password given by caller
   Security Rejection - Invalid Password given
   Security Rejection - HDLC not supported by the caller
   ```
   review the system configuration for the Device List. You can also refer to the *System Messages* chapter for the message meanings and the appropriate actions to be taken.

6. For IP Host Devices:
   If the system displays the following messages among the system messages:
   ```
   IP Call Dropped: ID_RSP was not received from remote
   IP Call Dropped: XID was not received from remote
   IP Security Rejection - Digit string wrong length
   IP Security Rejection - Invalid Security ID <Id string>
   ```

   Review the system configuration for the Device List. You can also refer to the *System Messages* chapter for the message meanings and the appropriate actions to be taken. The first two messages indicate that the system did not receive the required protocol data. The second two messages indicate that the security configuration is incorrect.

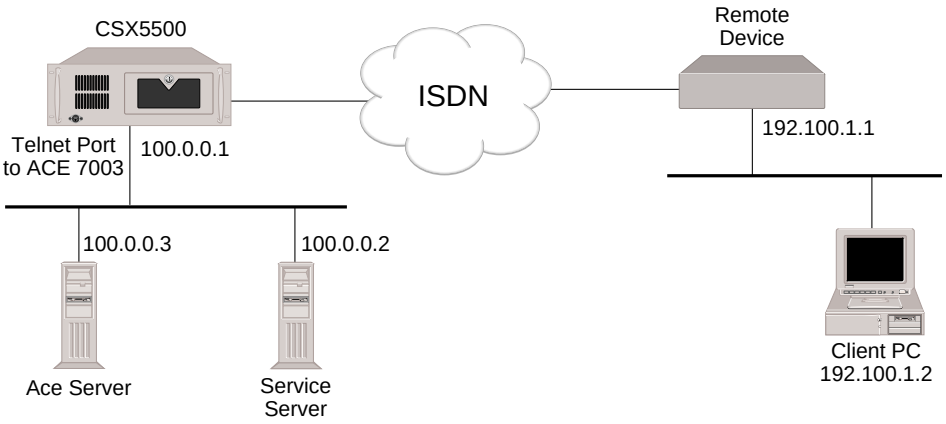
7. For PPP Devices:
   If the system displays any error or warning messages that begin with the following prefixes:
   ```
   [PAP].....
   [CHAP].....
   [AUTH].....
   ```

   There probably is an error in the remote device configuration. Review your remote device configuration. You can also refer to the *System Messages* chapter for the message meanings and the appropriate actions to be taken.

MULTI-LEVEL SECURITY

To verify device and user level security to the CyberSWITCH, the WAN lines that are connected to the system must be available for use, and IP, AppleTalk, or bridging options must be properly initialized. The remote devices must be operational and available to initiate ISDN WAN connections. The remote device must be configured on a device database, with User Level Authentication initially disabled. A client PC on the LAN of the remote device must a user ID and password for a user level database on an off-node server. Both databases must be enabled and available.

Below is an example of a configuration used to verify multi-level security over an IP WAN UnNumbered interface. It uses IP addresses specific to the example. Substitute the IP address of your network when you perform the multi-level security verification steps. It also uses the "ping" command. The "ping" command sends a packet to a specified host, waits for a response, and reports success or failure. Substitute the equivalent command on your network.



To verify multi-level security:

1. Determine if the client PC can ping the Service Server. On the Client PC, type:
   `ping 100.0.0.2` <return>

   If the ping is successful, then continue with the next step.

   If the client PC CANNOT ping to the Service Server, refer to *IP Routing over a WAN UnNumbered Interface Connection* in the *Verifying Routing Protocols* chapter.

2. Reconfigure the definition of the remote device in the device database to enable User Level Authentication. Attempt to ping the Service Server again. On the client PC, type:
   `ping 100.0.0.2` <return>

   If the ping is successful, disconnect the call. Ensure that User Level Authentication is enabled for the remote device, then try the ping again. The ping should fail.

   If the client PC CANNOT ping to the Service Server, then continue with the next step.

3. Telnet from the client PC into the central site. For example, telnet to 100.0.0.1, port 7003. Follow the normal user level authentication process.

4. Once again, determine if the client PC can ping the Service Server. On the Client PC, type:
   ping 100.0.0.2 <return>

   If the ping is successful, then multi-level security is operational.

5. If the ping is unsuccessful, *try the following:*
   a. Ensure that the remote device can ping across the network with User Level Authentication DISABLED.
   b. Disconnect the call if it is still up.
   c. Check to see if the User Level Security database and server are properly configured. Ensure that the user ID and password are accurate.
   d. If the problem is still not resolved, contact Customer Support.

IP HOST MODE

IP HOST INITIALIZED?

VERIFICATION

If you have configured the IP feature in the Host mode:

1. Determine if IP Host has been initialized by viewing the system messages. To view the messages, enter the following command:
   dr <return>

2. Look for the following IP message among the system messages:
   `[IP] IP Host is initialized successfully`

3. For the IP Interface that has been configured, the following interface initialization message should be displayed among the system messages:
   `[IP] Network initialized successfully on ddd.ddd.ddd.ddd`

   Note: Other messages may also be displayed with the IP router initialization messages.

   If you see these IP host initialization messages, then the IP host is operational.

4. If the system does not display the correct IP Host Initialization messages, or, instead, displays the following message:
   `[IP] IP Router is initialized successfully`

   a. Check the configuration. Make sure that the IP feature is enabled.
   b. Make sure that the operating mode is set to Host rather than Router.

IP HOST MODE OPERATIONAL?

To verify that IP Host mode feature is properly operational, a remote IP Host must be operational and available to initiate WAN connections via a remote bridge device. Also, a local IP host must be connected to the local LAN port on the CyberSWITCH.

Each section below uses example entries to verify IP Host mode operation. IP addresses are specific to the examples. Substitute the IP addresses of your network when you perform the IP Host mode feature verification steps. Each section also uses the *ip ping* command. The *ip ping* command sends a packet to a specified host, waits for a response, and reports success or failure. Substitute the equivalent command on your IP host.

VERIFICATION OVER A LAN CONNECTION

1. Determine if the CyberSWITCH can access the local IP host. Type:
   ip ping 100.0.0.2

2. If a message similar to the following is displayed, the IP host mode feature over the specified LAN port is operational. Repeat this step for each LAN port on your Ethernet resource.
   `100.0.0.2 is alive`

3. You may have a problem if you receive the message:
   `No response from <ip-address>`

   Try the following:

   a. Verify that the routing entry for the destination network exists by entering the following console command:
      iproute <ip-address>

   b. If the command returns "`No route is available for <ip-address>`", the routing entry does not exist. To correct, add the static routing entry using the *iproute add* Manage Mode command.

   c. Check that the CyberSWITCH and the specified Host both have the same Subnet mask and Sub network number for that ip-address using the *ipnetif* Manage Mode command. Correct the Host configuration, or the system configuration (using the *iproute change* Manage Mode command) as required.

   d. Verify that the ARP entry for the specified IP address exists. As required, ping from the IP Host so that the ARP entry is updated. Use the *ip arp* command to look at the ARP cache entries. (This command is described in the *System Commands* chapter.) If the ARP cache entry for the Host does not exist, verify that the Host is operational and that the CyberSWITCH and the Host are both physically connected to the same LAN segment.

   e. If the ARP cache entry exists for the Host, check that the IP Host has the same encapsulation type as the CyberSWITCH. The CyberSWITCH can receive and recognize either Ethernet or SNAP type encapsulations. Correct the IP Host or CyberSWITCH configuration (using CFGEDIT) for encapsulation type.

   f. Try to ping the Host from another device on the LAN. If this is also unsuccessful, this may indicate a problem with the Host.

   g. Verify that the hardware address (MAC address) for the IP Host in the CyberSWITCH's ARP cache is correct. If it is not correct, verify the configuration in the IP Host.

VERIFICATION OVER A WAN CONNECTION

1. Determine if a remote IP Host (Host B) can access the system. On the remote IP host type:
   ping 100.0.0.1

2. If a message similar to the following is displayed, the IP host mode feature over the specified WAN connection is operational.
   `100.0.0.1 is alive`

3. If this message is NOT displayed, then IP Host mode feature over the WAN connection is not operational. Try the following:
   a. Verify that the WAN connection is up. Use the *mc* command to check for the connection. If the connection is up, then continue with the next step.
   b. If the connection is NOT up, refer to *Remote Device Connectivity*.
   c. Follow the steps described in the section *IP Host Mode Operation Over the LAN Connection*.

ALTERNATE ACCESSES

DEDICATED CONNECTIONS

To verify a dedicated connection to the CyberSWITCH, the WAN lines that are connected to the system must be available for use, and the routing option must be properly initialized.

1. View the system messages by entering the following console command:
   dr <return>

2. Look for the following system message among the displayed messages:
   `Dedicated connection to device <device name> up: Slot=<slot#>, Port=<port #>`
   If the above message is displayed, the dedicated connection is functioning.

3. If you see either of the following messages, you may have a problem:
   `Layer 1 sync not seen - Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix>`
   `Dedicated connection down: Slot=<slot#>, Port=<port #>`

   Try the following:
   a. With the `Layer 1 sync not seen` message, a physical problem has been detected on the indicated line. Check for a proper connection to the CyberSWITCH and to the NT1 or CIU. If the NT1 or CIU appears to be functioning properly, call your carrier service and report the problem.

   b. With the `Dedicated connection down` message, a remote device could not be validated for some reason. Check the configuration for the device that will be using the dedicated connection.

   Refer to *Remote Device Connectivity*. Because all remote devices that use dedicated connections are PPP devices, follow the described set-up procedure, then skip to the step specific for PPP devices.

FRAME RELAY CONNECTIONS

To verify a frame relay connection to the CyberSWITCH, the WAN lines that are connected to the System must be available for use, and the routing option must be properly initialized. To verify a frame relay connection, perform the following:

1. Enter the *frame relay stats* command at the administration console.
   a. If the statistics display appears, the frame relay feature is configured and the frame relay subsystem should be operational.
   b. If you receive the message: `No Frame Relay Accesses configured,` verify your configuration. Refer to *Frame Relay Accesses* in the *Configuring Alternate Accesses* chapter.

2. Enter the *cs* command at the administration console. The device name for the associated PVC should appear in the list of connected sites.

3. Check the report log (*dr*) for additional messages. If you see any of the following, you may have a problem:

   ```
   Unexpected error during transmission of LMI frame
   [FR_IETF] Authentication Failure of remote device "NAME"
   [FR_IETF] Off-node Authentication Failure of remote device "NAME"
   ```

   Try the following:

   a. If the system displays the `Unexpected error during transmission of LMI frame` message: Use CFGEDIT to change the Frame Relay LMI type. Refer to *Configuring General Access Information* in the *Configuring Alternate Accesses* chapter.

   b. If the system displays one of the following messages:

   ```
   [FR_IETF] Authentication Failure of remote device "NAME"
   [FR_IETF] Off-node Authentication Failure of remote device "NAME"
   ```

   It indicates that the device database does not have a device entry corresponding to the permanent virtual circuit. Use CFGEDIT to change the PVC name to match the remote device name. Refer to *Configuring a PVC* in the *Configuring Alternate Accesses* chapter.

PPP LINK FAILURE DETECTION

To verify that Frame Relay's Link Failure Detection is enabled, perform a trace to view the Echo-Request and Reply packets:

1. With the feature enabled, establish a connection.

2. Erase the system log (*er* command).

3. Issue the *trace ppp on* console command.

4. Wait for at least the configured Echo Frequency.

5. Display the system log (*dr* command). If the feature is operational, some frames similar to the following will be displayed:

```
(I) 16:28:49.71 #C021: Conn=001 OUT-PPP:LCP      ECHO REQ Id=0x50 Len=10
(I) 16:28:49.71 #0000:   3E 03 78 AC
(I) 16:28:49.76 #C021: Conn=001 IN -PPP:LCP      ECHO RPLY Id=0x50 Len=10
(I) 16:28:49.76 #0000:   70 18 D0 87
(I) 16:28:59.82 #C021: Conn=001 OUT-PPP:LCP      ECHO REQ Id=0x51 Len=10
(I) 16:28:59.82 #0000:   3E 03 78 AC
(I) 16:28:59.82 #C021: Conn=001 IN -PPP:LCP      ECHO RPLY Id=0x51 Len=10
(I) 16:28:59.82 #0000:   70 18 D0 87
```

6. To determine if the feature detects a failure:

   a. Set up two systems in a back-to-back, dedicated, BRI scenario where at least one of the systems is a PC-Platform. Configure a dedicated access between the 2 systems.

      With the a PC-based platform, layer 1 of a BRI board stays active even when you exit the software. This gives us a way to simulate an end-to-end B-channel failure. That is, the only remaining way for the other system to detect the error is via the Link Failure Detection mechanism. (There are no D-channel failures or Layer 1 failures).

   b. On the non-PC system (or either of the two if both are PC-platforms), make sure that Link Failure Detection is enabled. Go to the *mc* screen to make sure that the dedicated connection is up.

   c. On the PC-platform system, enter the *quit* command.

   d. On the non-PC system wait for approximately the amount time of the echo frequency multiplied by the maximum attempts. At this time, the feature should detect the failure, and the *mc* screen should remove the dedicated connection.

   e. Check the log for the message which indicates that a link failure has been detected.

   f. If there is a failure, refer to *WAN Line Availability* for corrective actions.

X.25 CONNECTIONS

To verify an X.25 to the CyberSWITCH, the WAN lines that are connected to the System must be available for use, and the routing option must be properly initialized.

1. Enter the *x25 stats* command at the administration console. If the statistics display appears, the X.25 subsystem should be operational.

2. If the message: `No X.25 Accesses configured` is displayed, verify your configuration. Using CFGEDIT, verify that the proper line and port have been selected. If you are still having problems, try the following:

   a. Enter the *er* command to erase the report log.

   b. Enter the *trace lapb on* command.

c. Wait 20 seconds, then enter the *dr* command to display the report log. The status log should display a sequence of the following messages:

```
(I) 17:33:35.38 #1067: Out - LAPB RR, Rx Sequence = 1
(I) 17:33:35.38 #0000: 01 31 00 2A
(I) 17:33:35.38 #1067: IN - LAPB RR, Rx Sequence = 1
(I) 17:33:35.38 #0000: 01 31 A2 00
```

d. If these messages are not displayed, verify with the service provider that the line and bearer are provisioned for X.25 packet access, and the LAPB addressing format, modulo 8 or 128, is consistent with the line provisioning.

e. If the log contains a sequence similar to the following:

```
(I) 17:33:32.32 #1067: IN - LAPB SABM
(I) 17:33:42.32 #1067: IN - LAPB SABM
(I) 17:33:52.32 #1067: IN - LAPB SABM
```

verify with the service provider verify that the line and bearer are provisioned for X.25 packet access, and the LAPB addressing format, modulo 8 or 16, is consistent with the line provisioning.

f. If the log contains a sequence similar to the following:

```
(I) 17:33:32.32 #1067: IN - LAPB SABM
(I) 17:33:32.32 #0000: 03 3F A6 04
(I) 17:33:32.32 #1C05: x25 access 1 in state ACCESS UP for
    event LAPB UP
(E) 17:33:32.32 #1C04: Invalid event for access 1
(I) 17:33:32.32 #1C05: x25 access 1 in state ACCESS UP for
    event X25 DOWN
(I) 17:33:32.32 #1067: Out - LAPB UA
(I) 17:33:32.32 #0000: 03 73 00 10
```

verify that the LAPB timer values are consistent with the service provider specifications.

X.25 AND A TERMINAL SERVER MENU

1. If the CyberSWITCH is dialed, but the remote user does not get a menu, check configuration. Verify that *Use Menu for Authentication* is selected (*Security, Network Login, General Configuration, Terminal Server Security*).

2. If the CyberSWITCH is dialed and the modem connects, but the remote user does not get a menu or pad prompt, and then soon disconnects, check configuration. Verify that *X.3 PAD* is enabled (*Options*).

3. If the connection is made to the CyberSWITCH, and the menu / pad prompt is displayed, but keystrokes are not echoed: Verify correct pad parameter settings for non-transparent pad profile.

VERIFYING ROUTING PROTOCOLS

OVERVIEW

This chapter describes the verification process for the following CyberSWITCH routing protocols:

- *IP Routing*
- *IPX Routing*
- *AppleTalk Routing*

To perform the verification procedures, WAN lines must be available and ready to use. LAN attachment components must also be available and ready to use.

During some of the procedures, we ask you to enter an administration console command. To enter these commands, you must have an active administration session. If you need instructions for starting an administration session, refer to *Accessing the CyberSWITCH*. *Accessing the CyberSWITCH*.

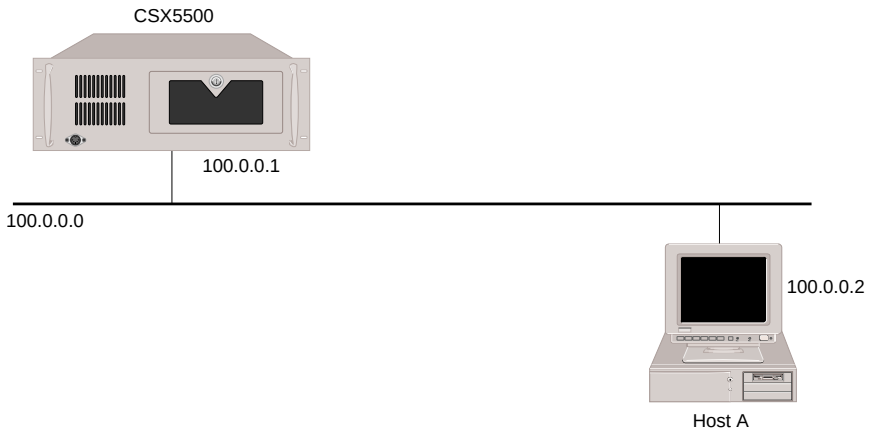
Note: At least one remote device is required to proceed with many of the verification procedures.

IP ROUTING OPERATIONAL?

IP ROUTING OVER A LAN INTERFACE

To verify that IP routing is operating properly over the LAN connection, an IP host must be connected to the local LAN port on the CyberSWITCH. The host must be properly configured and operational on the IP network to which it is connected.

Below is an example of a configuration used to verify IP routing over a LAN connection. It uses IP addresses specific to the example. Substitute the IP addresses of your network when you perform the IP routing verification steps.



1. Determine if the CyberSWITCH can access the local IP host. On the administration console type:

   ip ping 100.0.0.2 <return>

You should receive a response similar to the following:

```
100.000.000.002 is alive
```

If the system displays this message, then IP routing over that LAN port is operational. Repeat this step for each LAN port on your Ethernet resource.

2. If this message IS NOT displayed, then IP routing over the LAN connection is not operational. If you receive the following message:

```
No response from <ip-address>
```

Try the following:

a. Verify that the routing entry for the destination network exists. Enter the following administrative console command:

iproute <ip-address>

If the command returns "`No route is available for <ip-address>`", the routing entry does not exist. To correct, add the routing entry using the *`iproute add`* Manage Mode command.

b. Check that the system and the specified Host both have the same Subnet mask and Sub network number for that IP address using the *`ipnetif`* command (Manage Mode). Correct the Host configuration, or the system configuration (using the *`iproute change`* Manage Mode command) as required.

c. Verify that the ARP entry for the specified IP address exists. As required, ping from the IP Host so that the ARP entry is updated. Use the *`ip arp`* console command to look at the ARP cache entries. If the ARP cache entry for the Host does not exist, verify that the Host is operational and that the CyberSWITCH and the Host are both physically connected to the same LAN segment.

d. If the ARP cache entry exists for the Host, check that the IP Host has the same encapsulation type as the CyberSWITCH. The system can receive and recognize either Ethernet or SNAP type encapsulations. Correct the IP Host or system configuration (through CFGEDIT) for encapsulation type.

e. Try to ping the Host from another device on the LAN. If this is also unsuccessful, this may indicate a problem with the Host.

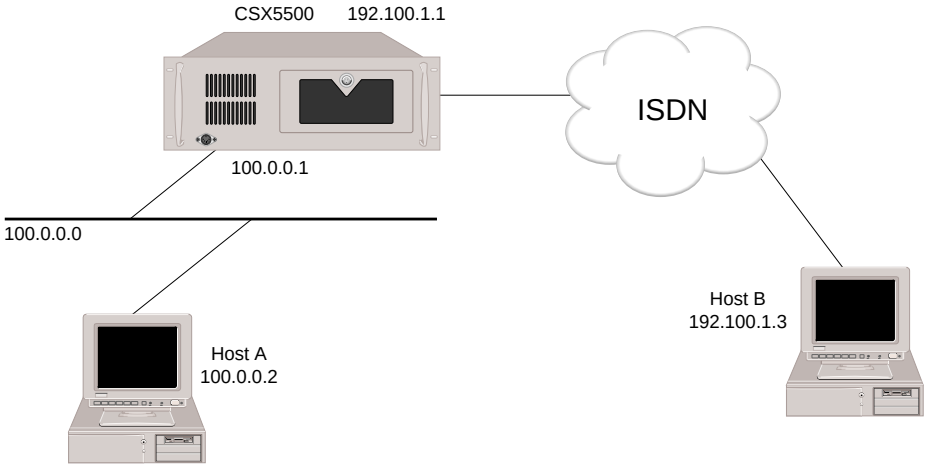
f. Verify that the hardware address (MAC address) for the IP Host in the system's ARP cache is correct. If it is not correct, verify the configuration in the IP Host.

Once IP routing is operational on each LAN port on your Ethernet resource, then IP routing over the LAN Connection is operational.

IP Routing Over a WAN Interface

To verify that IP routing is properly operational over a WAN interface, a remote IP Host must be operational and available to initiate connections. Also, a local IP host must be connected to the local LAN port of the CyberSWITCH.

Below is an example of a configuration used to verify IP routing over a WAN interface. It uses IP addresses specific to the example. Substitute the IP addresses of your network when you perform the verification steps. It also uses the "ping" command. The "ping" command sends a packet to a specified host, waits for a response, and reports success or failure. Substitute the equivalent command on your IP host.



1. Determine if a remote IP host can access the WAN interface of the CyberSWITCH over the WAN connection. On the remote IP host, type:
   `ping 192.100.1.1` <return>

   If the remote IP host successfully pings to the CyberSWITCH, continue with step 3.

2. If the remote IP host CANNOT ping to the system, *try the following*:
   a. Verify that the WAN connection is up. Use the `mc` console command to display the Connection Monitor display. Check for the connection. If the connection is up, continue with the next step.

      If the connection is NOT up, refer to the section titled *Remote Device Connectivity*.

   b. Verify that the WAN interface is properly initialized. Use the `ipnetif` command (Manage Mode) to check for the proper WAN interface. If it exists, continue with the next step.

      If the proper WAN interface does not exist, make corrections to the system configuration using CFGEDIT.

   c. Check that the IP address configured in the Device list for the IP Host device matches the address configured on the IP Host device. Make corrections to the CyberSWITCH's configuration (using the `iproute change` Manage Mode command), or to the IP Host's configuration, as required.

3. Determine if a remote IP host can access the LAN interface of the CyberSWITCH over the WAN connection. On the remote IP host type:
   `ping 100.0.0.1` <return>

   If the remote IP host successfully pings to the CyberSWITCH, then continue with the step 5.

4. If the remote IP host CANNOT ping to the CyberSWITCH, *try the following*:

   a. Verify that the LAN interface is properly configured by using the ***ipnetif*** command (a Manage Mode command).

      If the proper LAN interface does not exist, use CFGEDIT to make corrections.

   b. Verify that the remote IP Host is initiating a call to the CyberSWITCH. Since the LAN interface has an IP address assigned with a different network number than the one for the remote IP Host, the remote IP Host may need a proper route entry for the local network where the CyberSWITCH is located. Make corrections to the remote IP Host configuration.

5. Determine if a remote IP host can access the local IP host through the system over the WAN connection. On the remote IP host type:
   ping 100.0.0.2 <return>

   If the remote IP host successfully pings to the local IP host, then IP routing over WAN type interface is operational. Repeat steps 1 through 5 for each WAN type interface through which you wish to get access.

6. If the remote IP host CANNOT ping to the local IP host, *try the following*:

   a. Verify that the local IP Host has the route entry for the remote network with the CyberSWITCH as the next hop.

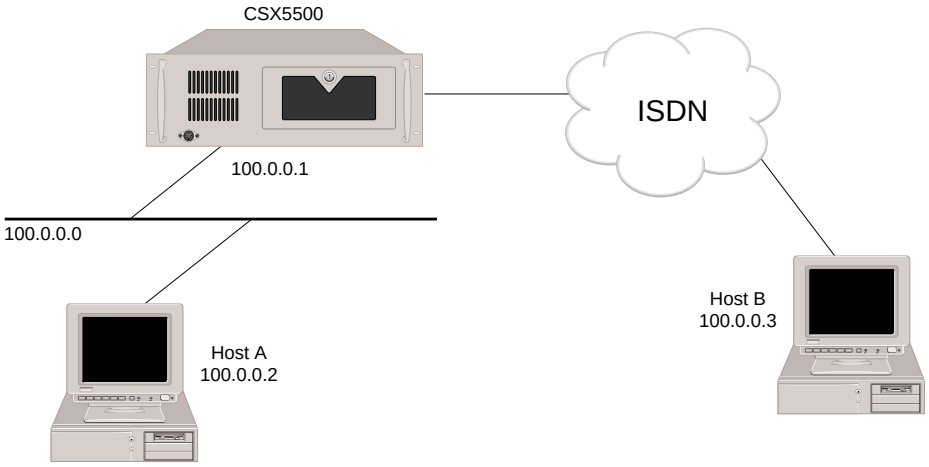
   b. If the local IP Host has the proper route entry to the remote network, refer to *LAN Connection* in the *Verifying Base System* chapter.

   c. If the local IP Host does not have the proper route entry, make corrections to the local IP Host configuration.

IP Routing Over a WAN (Direct Host) Interface

To verify that IP routing is properly operational over a WAN (Direct Host) interface, a remote IP Host must be operational and available to initiate connections. Also, a local IP host must be connected to the local LAN port on the CyberSWITCH.

Below is an example of a configuration used to verify IP routing over a WAN (Direct Host) interface. It uses IP addresses specific to the example. Substitute the IP addresses of your network when you perform the IP routing verification steps. It also uses the "ping" command. The "ping" command sends a packet to a specified host, waits for a response, and reports success or failure. Substitute the equivalent command on your IP host.



1. Determine if a remote IP host can access the CyberSWITCH over the WAN connection. On the remote IP host type:
   ping 100.0.0.1 <return>

   If the remote IP host successfully pings to the CyberSWITCH, continue with the step 3.

2. If the remote IP host CANNOT ping to the CyberSWITCH, try the following:
   a. Verify that the WAN connection is up. Use the *mc* console command to check for the connection. If the connection is NOT up, refer to *Remote Device Connectivity*.
   b. Verify that the WAN (Direct Host) interface is properly initialized. Use the *ipnetif* command (a Manage Mode command) to check for the proper WAN (Direct Host) interface. If the interface does NOT exist, use CFGEDIT to make corrections
   c. Verify that the subnet mask information and the IP address for the Remote Host matches the IP Host configuration.

3. Determine if a remote IP host can access the local IP host through the CyberSWITCH over the WAN connection. On the remote IP host type:
   ping 100.0.0.2 <return>

   If the remote IP host successfully pings to the local IP host, then IP routing over WAN (Direct Host) interface is operational. Repeat the above steps for each WAN (Direct Host) interface you wish to access.

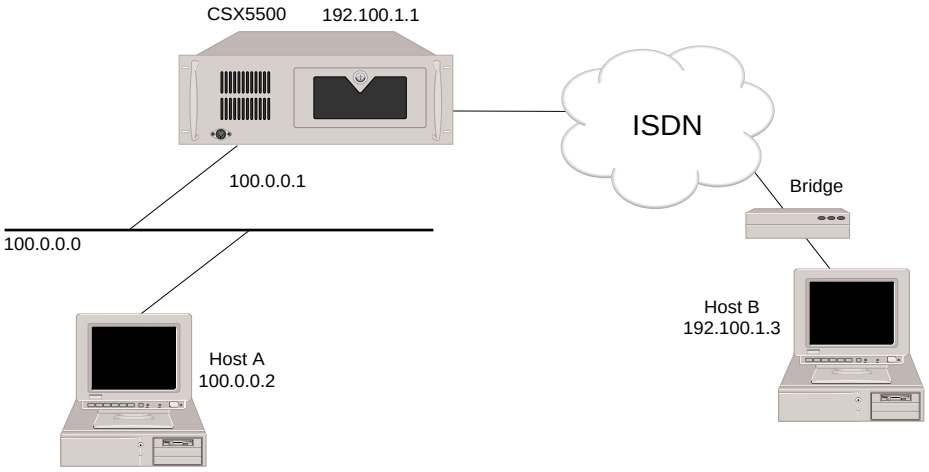
4. If the remote IP host CANNOT ping to the local IP host, try the following:

   Verify that the remote IP Host can access the LAN interface of the CyberSWITCH, since the remote IP Host connected to a WAN (Direct Host) interface should be recognized as if it were located on the local Ethernet. Refer to the *Verifying IP Routing Over a LAN Interface* section for more information.

IP ROUTING OVER A WAN REMOTE LAN INTERFACE

To verify that IP routing is properly operational over a WAN Remote LAN interface, a remote IP Host must be operational and connected to the remote LAN. The remote bridge device must be operational and available to initiate connections. Also, a local IP host must be connected to the local LAN port on the CyberSWITCH.

Below is an example of a configuration used to verify IP routing over a WAN Remote LAN interface. It uses IP addresses specific to the example. Substitute the IP addresses of your network when you perform the IP routing verification steps. It also uses the "ping" command. The "ping" command sends a packet to a specified host, waits for a response, and reports success or failure. Substitute the equivalent command on your IP host.



1. Determine if a remote IP host can access the WAN Remote LAN interface of the CyberSWITCH over the WAN connection. On the remote IP host type:
   `ping 192.100.1.1` <return>

   If the remote IP host successfully pings to the CyberSWITCH, continue with step 3.

2. If the remote IP host CANNOT ping to the CyberSWITCH, try the following:

   a. Verify that the WAN connection is up. Use the *mc* console command to display the Monitor Connections screen. Check for the connection. If the connection is NOT up, refer to *Remote Device Connectivity*.

   b. Verify that the WAN RLAN interface is properly initialized. Use the *ipnetif* command (a Manage Mode command) to check for the proper WAN RLAN interface. If the proper interface does NOT exist, use CFGEDIT to make the necessary corrections.

   c. Check that the IP address configured in the Device list for the IP Host device matches the address configured on the IP Host device. Make corrections to the CyberSWITCH's configuration (using the *iproute change* Manage Mode command), or to the IP Host's configuration, as required.

3. Determine if a remote IP host can access the LAN interface of the CyberSWITCH over the WAN connection. On the remote IP host type:
   ping 100.0.0.1 <return>

   If the remote IP host successfully pings to the CyberSWITCH, then continue with step 5.

4. If the remote IP host CANNOT ping to the CyberSWITCH, try the following:
   a. Verify that the remote IP Host can access the WAN RLAN interface of the CyberSWITCH.

   b. Verify that the LAN interface is properly initialized. Use the *ipnetif* command (a Manage Mode command) to check for the proper LAN interface. If the proper interface does not exist, use CFGEDIT to make the necessary corrections.

   c. Verify that the remote bridge device is initiating a call to the CyberSWITCH. Since the CyberSWITCH LAN interface has an IP address assigned with a different network number than the one for the remote IP Host, the remote IP Host may need a proper route entry for the local network where the CyberSWITCH is located. Make corrections to the remote IP Host configuration.

5. Determine if a remote IP host can access the local IP host through the CyberSWITCH over the WAN connection. On the remote IP host type:
   ping 100.0.0.2 <return>

   If the remote IP host successfully pings to the local IP host, then IP routing over the WAN Remote LAN interface is operational. Repeat the above steps for each WAN Remote LAN interface you wish to access.

6. If the remote IP host CANNOT ping to the local IP host, try the following:

   a. Verify that the remote IP Host can access the LAN interface of the CyberSWITCH. If it cannot, refer to the *IP Routing Over a LAN Interface* section for more information.

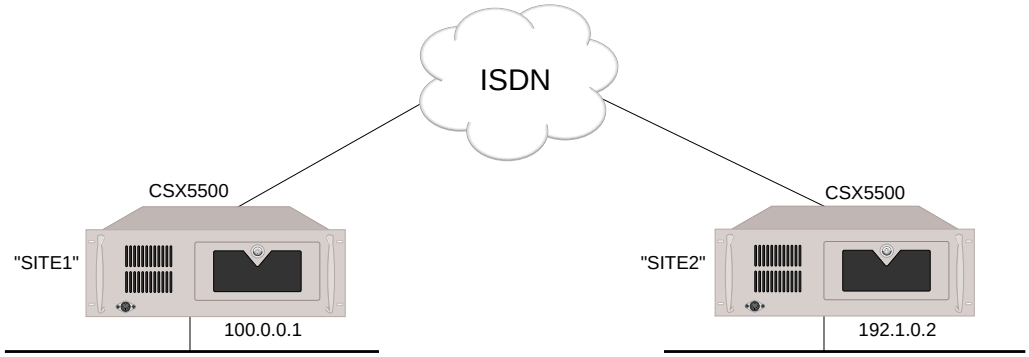
   b. Verify that the local IP Host has the route entry for the remote network with the CyberSWITCH as the next hop. If it does, refer to the *LAN Connection* section in the *Verifying Base System* chapter.

   If the local IP Host does NOT have the proper route entry, make corrections to the local IP Host configuration.

IP ROUTING OVER A WAN UNNUMBERED INTERFACE

To verify that IP routing is properly operational over a WAN UnNumbered interface, the CyberSWITCH must be operational and available to initiate connections.

Below is an example of a configuration used to verify IP routing over a WAN UnNumbered interface. It uses IP addresses specific to the example. Substitute the IP addresses of your network when you perform the IP routing verification steps. It also uses the “ping” command. The “ping” command sends a packet to a specified host, waits for a response, and reports success or failure.



1. Determine if SITE1 can access SITE2 over the WAN connection. On system A type:
   ip ping 192.1.0.2 <return>

2. Determine if system B can access system A over the WAN connection. On system B type:
   ip ping 100.0.0.1 <return>

3. If the systems CANNOT ping each other, *try the following*:

   a. Have the remote router ping itself using its LAN IP address.
   b. Have the CyberSWITCH ping itself using its LAN IP address.
   c. Have the router ping the CyberSWITCH. If the ping is unsuccessful:
      - and no call is up, check the static route on the router
      - and a call is up, check the static route on the CyberSWITCH.

IP FILTERS

1. Configure and apply at least one IP filter that contains at least one condition whose action is to DISCARD the matching packet.

2. Perform a trace on discarded packets. On the administration console issue the command:
   ip filter trace discard <return>

3. Attempt to transfer data that would be affected by the configured filters. Be sure to include packets which should be discarded by the configured filters.

4. Check the report log for discarded packets. Issue the administrative console command:
   dr <return>

   If IP Filters are discarding packets, the report log will display [IPFILT] messages similar to the following:

```
9A00:          [IPFILT] UDP/1 at Intf. lan/Out
9A00:          {IP} Src: 128.131.0.1   Dst: 128.131.0.7   Pr:17
9A00           {UDP} Src:5001   Dst:69
```

5. If no packets have been discarded, check to see if the filters are properly configured. *Try the following*:

   a. From Manage Mode, issue the *ipfilt* command. Check the configured packet types, as well as the configured filters:
      - For *packet types*, it is important to verify that the contents of the packet in question are indeed correctly specified (IP Addresses, Protocol, TCP Ports, etc.).
      - For *configured filters*, keep in mind that component conditions are executed in the order in which they appear in the configuration. It is possible that a packet is not being discarded as expected if a previous condition matches that packet with an action of forward.

   b. Check to see if the filters are properly applied:
      - For global filters, use Manage Mode's *ipfilt* command. Check the *Apply Global Forwarding Filter* option.
      - For filters applied on a per-device basis, use Manage Mode's *device* command. Check to see if filters properly applied.
      - For network interface filters, check the IP interface information in CFGEDIT (*Options, IP Configuration, IP Interface)*.

   c. Make configuration changes as necessary.

6. *If you are still experiencing problems:*

   a. Check the status of the Exception Filter (using Manage Mode, *ipfilt* command). The Exception Filter overrides all other filters. If the Exception Filter is enabled, this could be the problem.

   b. With per-device and network interface filters, it is necessary that the packet in question truly flows through the desired application point. Try this test:
      - Disable the per-device and network interface filters.
      - Apply each filter in question *globally*.
      - When desired IP packets are received, it is guaranteed that they will pass through the filter in question. You can then analyze the effects in isolation. Your findings will be helpful if you need to call Customer Support.

7. If the IP filters are properly configured, and the system is still not correctly discarding packets, contact Customer Support.

8. When test completed, turn off the trace. Issue the administrative console command:
   ip filter trace off <return>

IP RIP INITIALIZED?

1. Determine if IP RIP processing has been initialized by viewing the system messages. On the administration console type:
   `dr` <return>

2. The `dr` command displays the current system messages. Look for the following IP RIP message among the system message:
   `[IP RIP] RIP Protocol Initialization successful`

If you see this IP RIP initialization message, the IP RIP has initialized successfully.

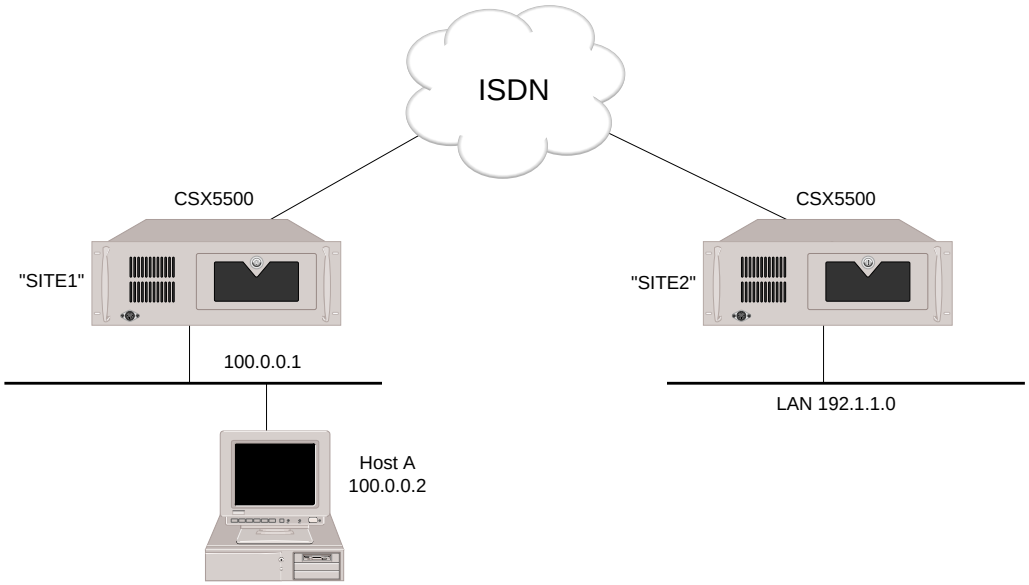
3. If the CyberSWITCH does not display the correct IP RIP Initialization message, and instead, displays one or more of the following messages:
   ```
   [IP RIP] Initialization failed, unable to allocate buffers
   [IP RIP] Unable to open RIP/UDP port 512
   ```
   There may be an a problem within the software. Contact Customer Support.

IP RIP Output Processing on a LAN Interface

To verify that IP RIP Output Processing (routes advertisement) is properly operational on a LAN interface, the IP RIP processing must be successfully initialized. Also, a local IP host (router) must be connected to the local LAN port on the system and capable of learning routes information via RIP.

Below is an example of a configuration used to verify IP RIP output processing on a LAN interface. It uses IP addresses specific to the example. Substitute the IP addresses of your network when you perform the verification steps. It also uses the *`netstat`* administration console command. The *`netstat`* command displays the IP routing table of the system. Substitute the equivalent command on your IP host.

.



1. Make sure that a static route to the network 192.1.1.0 is configured on SITE1. On SITE1's administration console type:
   `ip route` <return>

   If the route to 192.1.1.0 is displayed continue with step 3.

2. If the route is NOT displayed, use the Manage Mode command *`iproute add`* to add the static route.

3. Determine if a local IP Host A has learned the route to 192.1.1.0 from System A. On IP Host A type:
   netstat -r <return>

   If the route to 192.1.10 is displayed, the IP RIP output processing is operational.

4. If the route is NOT displayed, *try the following*:

   a. Using the *ipnetif* Manage Mode command, verify that the IP RIP Send Control is set to a RIP version that the IP Host can understand.

   b. If the command shows `Do Not Send`, the IP RIP output processing is disabled on the interface. Correct the RIP Send Control configuration using CFGEDIT.

   c. If the command shows an improper version of RIP, correct the RIP Send Control to the proper RIP version that the IP Host can understand.

5. Enter the *ip rip stats* administrative console command. Look for the `IfStatSentResponses` counter for the interface, which shows the number of RIP update messages sent on the interface.

   a. If the counter is 0, enter the *ip rip send* administrative console command to force the RIP update message to be sent immediately.

   b. Reissue the *ip rip stats* command.

   c. If the counter is still 0, there is an unexpected condition present within the CyberSWITCH software. Contact Customer Support.

6. If the RIP Send Control is set to "RIP Version 1" or "RIP Version 1 Compatibility," use Manage Mode to verify that the transmit broadcast address on the interface is set to a proper address that the IP Host can receive (through issuing the *ipnetif* Manage Mode command).

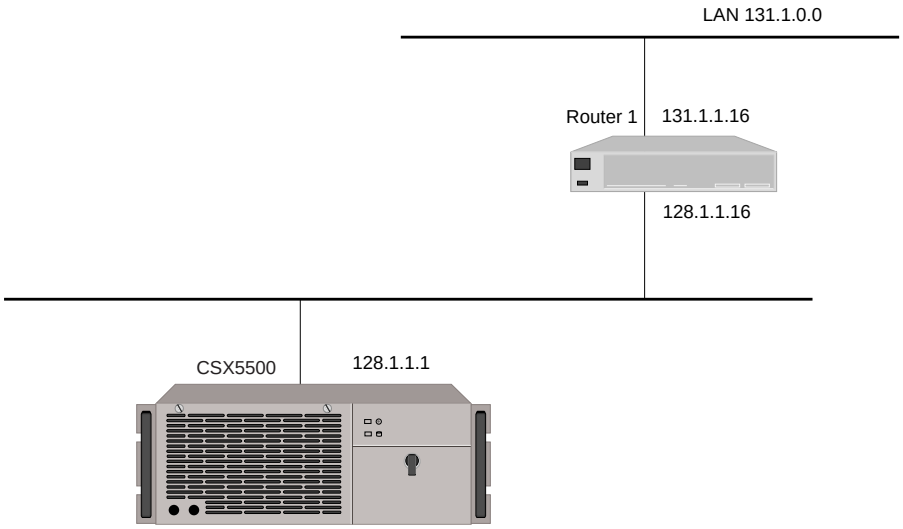
7. If the transmit broadcast address is not set properly, use CFGEDIT to correct it.

8. Check the IP Host and ensure that it is set up to learn route information via RIP.

IP RIP INPUT PROCESSING ON A LAN INTERFACE

To verify that IP RIP Input Processing (routes learning) is properly operational on a LAN interface, IP RIP processing must be successfully initialized. Also, a local IP router must be connected to the local LAN port on the system and capable of propagating routes information via RIP.

Below is an example of a configuration used to verify IP RIP input processing on a LAN interface. It uses IP addresses specified to the example. Substitute the IP addresses of your network when you perform the verification steps. It also uses the *netstat* command. The *netstat* command displays the IP routing table of the system. Substitute the equivalent command on your IP router.



1. Determine if the CyberSWITCH has learned the route to 131.1.0.0 from Router 1. On the administration console type:
   ip route <return>

   If the following route entry is displayed among other route entries, the IP RIP input processing is operational. The 'P' (Protocol) field should have 'R', which indicates that the entry was learned via RIP.

```
Destination     Subnet-Mask     Next Hop     Mtr T/P TTL IF AGE
131.1.0.0       255.255.0.0     128.1.1.16    1   R/R 999   n nnn
```

2. If the route is NOT displayed, *try the following*:

   a. Verify that the IP RIP Receive Control is set to the proper RIP version that the Router is using. Refer to page 443 for instructions regarding check RIP versions.

   b. Enter the *ip rip stats* administrative console command. Look for the counter `IfStatRcvResponses` for the interface, which show the number of RIP update messages received on the interface. If the total number of these counters is 0, check the Router to verify that it is configured to send IP RIP update messages.

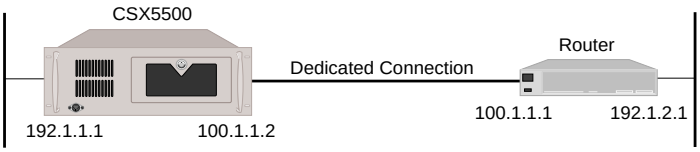
   c. Also look for the `IfStatRcvBadPackets` and `IfStatRcvBadRoutes` counters.
      - If these counters are not 0, there may be something wrong with the Router.
      - If these counters are 0, there is an unexpected condition present within the CyberSWITCH software. Contact Customer Support.

IP RIP Output Processing on a WAN Interface

To verify that IP RIP Output Processing (routes advertisement) is properly operational on a WAN interface, the IP RIP processing must be successfully initialized.

Below is an example of a configuration used to verify IP RIP output processing on a WAN interface. It uses IP addresses specific to the example. Substitute the IP addresses of your network when you

perform the verification steps. It also uses the *show ip route* command. The *show ip route* command is used by a specific router to display the IP routing table. Substitute the equivalent command for your IP router.



1. Make sure that a dedicated connection between system and Router is up and operational. On the system's administration console:
   Type: *cs*<return>

2. Determine if Router has learned the route to 192.1.1.0 from the system. On the Router:
   Type: *show ip route*<return>

   If the route to 192.1.1.0 is displayed, the IP RIP output processing is operational.

3. If the route is NOT displayed, *try the following*:

   a. Verify that the IP RIP Send Control is set to the proper RIP version that the Router can understand. Refer to page 443 for instructions regarding check RIP versions.

   b. Enter the *ip rip interface* administrative console command. Look for the ***Broadcast Address*** value. This is the IP address of the router that the RIP messages are sent to.

   c. If the address is not the correct address for the Router, correct the transmit broadcast address for the interface using CFGEDIT. Refer to page 443 for instructions regarding checking the address.

4. Enter the *ip rip stats* administrative console command. Look for the ***IfStatSentResponses*** counter for the interface, which shows the number of RIP update messages sent on the interface.

   a. If the counter is 0, enter the *ip rip send* administrative console command to force the RIP update message to be sent immediately.

   b. Reissue the *ip rip stats* command. If the counter is still 0, there is an unexpected condition present within the CyberSWITCH software. Contact Customer Support.

5. Check the Router and ensure that it is set up to learn route information via RIP.

IP RIP INPUT PROCESSING OPERATIONAL ON A WAN INTERFACE

To verify that IP RIP Input Processing (routes learning) is properly operational on a WAN interface, the IP RIP processing must be successfully initialized.

The same example that is used in the previous section is used to verify IP RIP input processing on a WAN interface.

1. Make sure that a dedicated connection between system and Router is up and operational. On the CyberSWITCH administration console:
   Type: *cs*<return>

2. Determine if system has learned the route to 192.1.2.0 from the Router. On the CyberSWITCH administration console:
   Type: *ip route*<return>

   If the route to 192.1.2.0 is displayed, the IP RIP input processing is operational.

3. If the route is NOT displayed, *try the following*:

   a. Verify that the `IP RIP Receive Control` is set to the proper RIP version that the Router is using. Refer to page 443 for instructions regarding check RIP versions.

   b. Enter the *ip rip stats* administration console command. Look for the ***IfStatRcvResponses*** counter for the interface. This statistics is the number of RIP update messages received on the interface. If the total number of these counters is 0, check the Router to verify that it is configured to send IP RIP update messages.

   c. Also look for the *IfStatRcvBadPackets* and *IfStatRcvBadRoutes* counters.
      - If these counters are not 0, there may be something wrong with the Router.
      - If these counters are 0, there is an unexpected condition present within the CyberSWITCH system software. Contact Customer Support.

IPX

IPX ROUTER INITIALIZED?

1. Determine if IPX routing has been initialized on the CyberSWITCH by viewing the system messages. To display the messages enter the following console command:
   dr <return>

2. Look for the following IPX message among the system messages:
   `[IPX] IPX router is initialized successfully`

   Also, for each IPX interface that has been configured, the following interface initialization message should be displayed among the system messages.
   `[IPX] Network initialized successfully on xxxxxxxx:xxxxxxxxxxxx`

   Note: Other messages may also be displayed with the IPX router initialization messages.

   If you see these IPX router initialization messages, the IPX router is initialized.

3. If these IPX router initialization messages are NOT displayed, look for the following message:

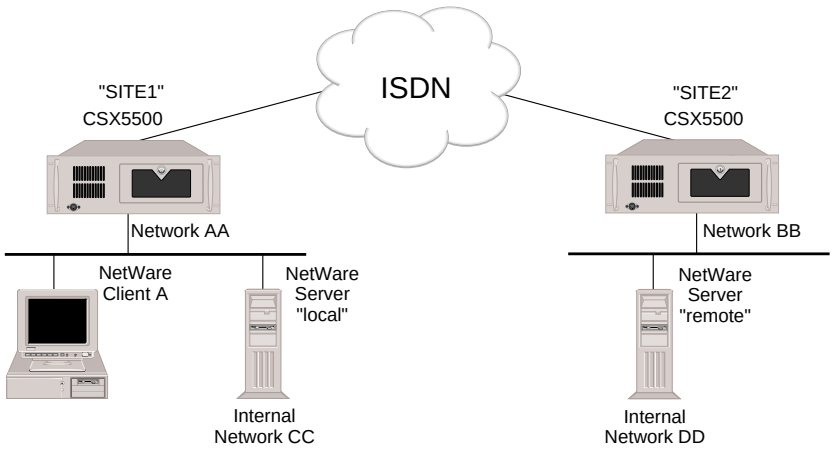
   `[IPX] Initialization failure`

   This message indicates an internal error. Contact Customer Support

IPX ROUTING OPERATIONAL?

To verify that IPX routing feature is properly operational, a local NetWare client, a local NetWare server and a remote NetWare server must be operational.

The following graphic illustrates an example network we will use to describe how to verify that IPX routing is operational. It uses IPX network addresses specific to the example. Substitute the IPX network numbers of your network when you perform the verification steps. The example also uses NetWare commands available for the Windows 95 workstation. Substitute the equivalent commands on your NetWare client.



IPX ROUTING OVER A LAN CONNECTION

1. Determine if SITE1 can access the local NetWare Server “local.” On SITE1’s administration console type:

   ```
   ipx diag cc:1 <return>
   ```

   Note: Node address 1 is used by the NetWare servers as part of their internal address.

2. If the system displays a response to the *ipx diag* command similar to:

   ```
   received 3 components from cc:1
   ```

   then IPX routing over that LAN port is operational.

3. If this message is NOT displayed, then IPX routing over the LAN connection is not operational and the following message will most likely be displayed:

   ```
   No response from <ipx-address>
   ```

   a. Verify that the routing entry for the destination network exists by entering the following console command:

   ```
   ipx route
   ```

   If the CyberSWITCH displays the route to the destination, it knows how to reach the local server’s internal network. Determine if this is a static route or a dynamic route learned via

RIP. The output of an *ipx route* command contains a protocol (P) field for each route entry, which indicate if it is static (L- locally configured) or dynamically learned via RIP (R). If it is learned via RIP, then basic communication between the CyberSWITCH and the local NetWare server is operational, and it is uncertain why the NetWare server does not respond to the ping request. Contact Customer Support.

b. Verify that RIP protocol is enabled by entering the following Mange Mode command:
ipxrip

Enable RIP if it is not already enabled.

c. Using the *ipxnetif* Manage Mode command, verify that IPX RIP send and receive control is enabled for the LAN interface.

Using CFGEDIT (under IPX network interfaces) enable RIP send and receive control if it is not already enabled.

d. If the route does not exist, or the route is a static entry, then verify that the CyberSWITCH and the local NetWare server are using the same packet encapsulation. To check the type of encapsulation, use the *ipxnetif* Manage Mode command. If they are not using the same encapsulation, then correct it either on the CyberSWITCH or the NetWare server.

e. Verify that the CyberSWITCH and the NetWare server are using the same external IPX network number for their mutual LAN (AA for this example). To check the network number that the CyberSWITCH is using, use the *ipxnetif* Manage Mode command. If they are not using the same external network number, then correct the problem.

IPX REMOTE LAN CONNECTION

To verify that IPX routing is properly operating over a WAN Remote LAN interface, a remote IPX router (e.g., SITE1) must be operational and connected to the Remote LAN. The remote bridge device (e.g., SITE2) must be operational and available to initiate connections.

1. From the router (SITE1), verify that the IPX Remote LAN interface has initialized. On the router's administration console type:
dr

You should see messages stating that the IPX network has initialized successfully on *xxxx*. Verify that "*xxxx*" is the network number of the Remote LAN.

2. If the system does NOT display the IPX messages indicating successful initiation, *try the following*:

Check the IPX network interface configuration. Refer to *Configuring IPX Network Interfaces* for details.

3. Determine the router's (SITE1) MAC address. From the router, issue the command:
ver

4. From the remote bridge (SITE2), attempt to access the IPX router by issuing the following administration console command:
   `ipx diag xxxx:yyyyyyyyyyyy`

   where: *xxxx* is the IPX Network Number
   yyyyyyyyyyyy is the router's MAC address

   If connection is up, host sends a message in response to this packet to confirm receipt.

   Note: The *ipx diag* and the *ipx ping* commands both test device connectivity (although both send back different types of responses). However, due to the variety of vendors and equipment available to networks, one command may work with a particular vendor or file server, while the other may not. If you are not experiencing success with *ipx diag*, try *ipx ping*, and vice versa.

5. If the CyberSWITCH does not recognize an ipx diag packet from the Remote Bridge, check IPX device information configuration. Refer to *Remote LAN Devices* for details.

6. Verify the call has come up. From the router side (SITE1), issue the following administration console command to display the monitor connections screen:
   `mc`

   If the call is displayed on the monitor connections screen, the IPX Remote LAN interface is operational.

7. If the call is NOT displayed, or you are experiencing data transfer problems, *try the following*:

   a. If data is not forwarded from the remote bridge to the router, check the configuration:
      - Verify Remote LAN interface configuration. Refer to *Configuring IPX Network Interfaces* for details.Verify device configuration on remote bridge. Bridge devices should be configured to make calls over the interface defined to go to the router.

   b. If the router does not forward typical data (RIP, SAP, Type 20 packets) to the remote bridge:
      - Make sure a call is up. Remember, the router cannot forward data if there is no previous connection (i.e., router currently does not support dial-out).
      - Check IPX device information on the router side. Refer to *Remote LAN Devices* for details.

   c. If the call does come up between the router and the remote bridge, but data is NOT received by a remote client (or server), try the following:
      - Double check and resolve any configuration/connection problems for the client (or server) to the bridge on the Remote LAN. (Basically, eliminate the possibility of any LAN configuration problems which are unrelated to the Remote LAN interface).
      - If you determine the problem is related to the Remote LAN, verify the IPX Network Number for the remote bridge in the router's configuration (under bridging properties). Refer to *Remote LAN Devices* for details.

IPX ROUTING OVER A WAN CONNECTION

1. Determine if NetWare Client A can see the remote NetWare Server "remote." To do this, activate NetWare Client A's desktop network neighborhood feature. Then check to see if "remote" is included in Client A's network neighborhood.

2. If "remote" is included in Client A's network neighborhood, them IPX over the WAN connection is operational. If it does not appear in the network neighborhood, then IPX over the WAN connection is not operational. *Try the following:*

   a. Verify that the routing entry for the remote NetWare's internal network exists by entering the following command.

      ```
      ipx route
      ```

      If the route entry does not exist, add a static route to it using the ***ipxroute add*** command (Manage Mode) because no route information (RIP packets) are exchanged over the WAN connections.

   b. Verify that the proper service entries of the remote NetWare server exist by entering the following console command:

      ```
      ipx service
      ```

      If the proper service entries do not exist, add static services using the ***ipxservice*** command (Manage Mode) because no service information (SAP packets) are exchanged over the WAN connections.

   c. Verify that the CyberSWITCH has SAP processing enabled for the LAN interface by using the ***ixpnetif*** command (Manage Mode). If the SAP processing is not enabled, change the configuration for the network interface.

TRIGGERED RIP/SAP

1. Determine if triggered RIP / SAP has started by viewing the system messages. To display the messages, enter the following console command:

   ```
   dr <RET>
   ```

2. Look for following message among the system messages:

   ```
   Starting Triggered RIP/SAP for <WAN Peer>
   ```

3. If this message is not displayed, *try the following*:

   Verify that the WAN peer is properly configured. Issue the *device* command in Manage Mode to display the current Device List. Or, you may view the WAN peer list through CFGEDIT, *Options*, *IPX Configuration*, *Triggered RIP/SAP*. Be sure that the device (WAN peer) has IPX routing enabled and triggered RIP / SAP (active) selected as routing protocol.

4. Determine if triggered RIP is operational. On the administration console, type:

   ```
   ipx trigrip stats
   ```

5. Examine statistics for activity. Refer to *Triggered RIP Statistics* for possible statistics and their descriptions.

6. Create a change in the route (for example, shut down a server). Again examine statistics (*`ipx trigrip stats)`* to verify the change is propagated to other side.

7. If statistics do not reflect change, *try the following*:

   a. Verify triggered RIP / SAP has successfully started for peers. Issue the *`dr`* console command and look for the "starting" message in the log.
   b. Generate a triggered RIP / SAP update request to the devices in question. Issue the following console command for each device:
      `ipx trigreq <device>`

   c. Verify that the statistics are incremented properly. Issue the following console commands:
      `ipx trigrip stats`
      `ipx trigsap stats`

   d. If routes / services are not propagated on either side, contact Customer Support.

8. Check routing table statistics. Issue the command:
   `ipx route stats`

   If the routing table on the CyberSWITCH is full, you will need to adjust your configuration. Note the following:

   The number of entries in the routing table is a configurable entity. This parameter may be between the values of 20 and 3072, and should be based on system need and system memory constraints. We recommend this value be at least 10% more than what you predict to be needed (more than 10% with larger network topologies). To predict need, use the following formula:

   1 + (2 x # configured IPX network interfaces) + (# configured static routes) + (# RIP routes)

   a. Determine number of needed entries in routing table:
      - Issue the *IPX route stats* command to determine number of configured static routes and RIP routes;
      - from Manage Mode, issue *ipxnetif* command to determine number of network interfaces;
      - plug this data into previously-described formula.

   b. Run *CFGEDIT*. From *Options*, select *IPX Routing.*

   c. Select *IPX RIP Table maximum number...*

   d. Increase the size of the table based upon your calculations.

9. Check the service table statistics. Issue the command:
   `ipx service stats`

10. If the service table on the CyberSWITCH is full, you will need to adjust your configuration. Note the following:

    The number of entries in the service table is a configurable entity. This parameter may be between the values of 20 and 3072, and should be based on system need and system memory

constraints. We recommend this value be at least 10% more than what you predict to be needed (more than 10% with larger network topologies). To predict need, use the following formula:

(# configured static services) + (# SAP services)

a. Determine number of needed entries in service table:
   - Issue the *IPX service stats* command to determine number of configured static services and SAP services;
   - plug this data into previously-described formula.

b. Run *CFGEDIT*. From *Options*, select *IPX Routing.*

c. Select *IPX SAP Table maximum number...*

d. Increase the size of the table based upon your calculations.

APPLETALK ROUTING

APPLETALK ROUTING INITIALIZED?

1. Determine if AppleTalk routing has been initialized on the CyberSWITCH by viewing the system messages. To view the system messages, enter the following console command:
   ```
   dr
   ```

2. Look for the following message among the system messages:
   ```
   AppleTalk routing initialized successfully
   ```

3. For the AppleTalk port that has been configured, the following port initialization message should be displayed among the system messages:
   ```
   AppleTalk successfully initialized on <port-type> with address
   <net.node>
   ```

   Note: `<port-type>` is either LAN port 1, LAN port 2 or WAN.
   `<net.node>` is the AppleTalk address assigned to this port.

4. If you see these AppleTalk routing initialization messages, then the AppleTalk routing has initialized properly.

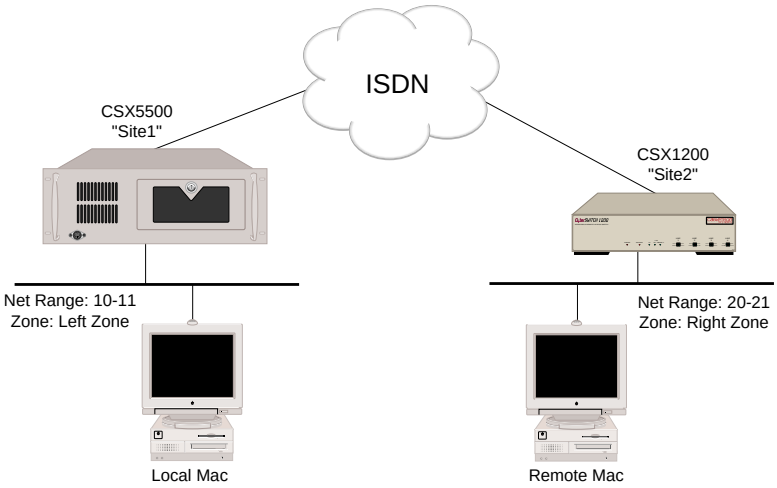
5. If these messages are NOT displayed, *try the following*:

   Check the system configuration. Make sure that the AppleTalk feature is enabled for the system.

APPLETALK ROUTING OPERATIONAL?

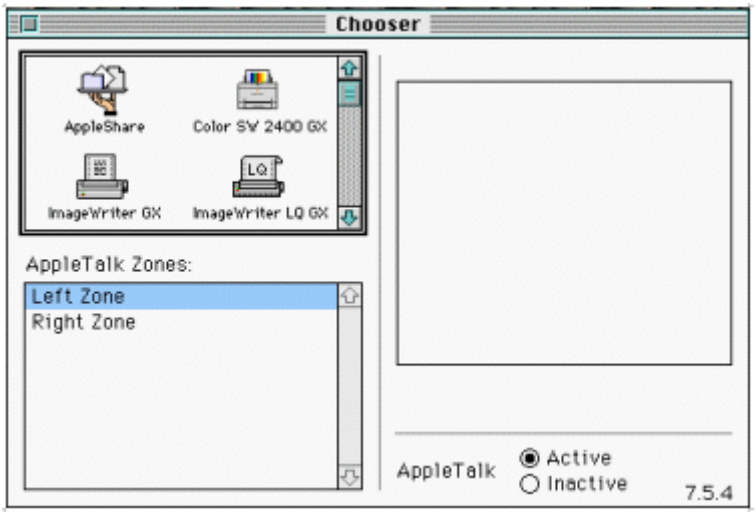
To verify that AppleTalk routing is properly operational, a remote Macintosh must be operational and available to initiate WAN connections via a remote AppleTalk router device. Also, a local Macintosh device must be connected to the local LAN port on the CyberSWITCH.

Below is an example of a configuration used to verify AppleTalk Routing operation. It uses AppleTalk addresses, zones and resource names specific to the example. Substitute those of your network when you perform the AppleTalk Routing feature verification steps.



APPLETALK ROUTING OVER THE LAN CONNECTION

1. Determine if the local Macintosh can see all zones. Bring up the Chooser on the Local Mac:



2. If a list of all zones (*Left Zone* and *Right Zone*) appear in the Chooser as shown above, then the AppleTalk Routing over a LAN connection is operational. Continue with the next step.

3. If all zones are NOT displayed, then AppleTalk Routing over the LAN connection is not operational, *try the following*:

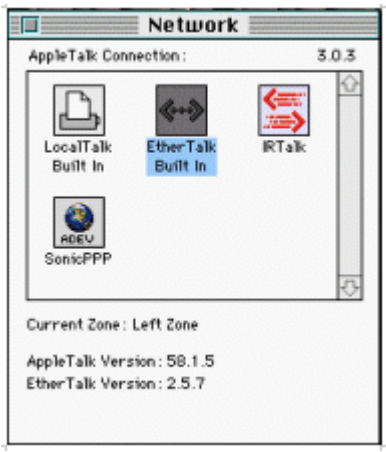
a. Verify that the AppleTalk LAN port that Local Mac is attached to is in *up state* by entering the following console command:

```
atalk port
```

b. If the command shows the port is not in up state, wait for a couple of minutes and repeat this step.

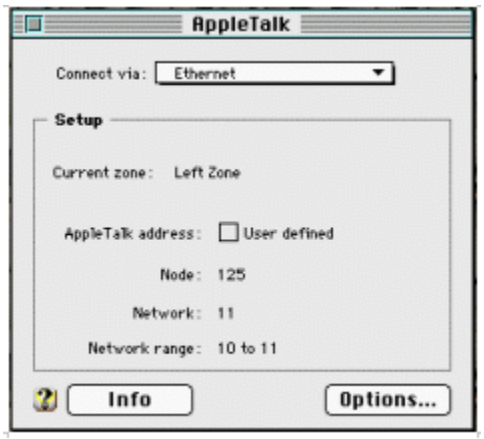
c. Check to see if the LAN connection of the port is operational. If the LAN connection is not operational, then correct the problem.

d. If you are using Classic Networking, verify that EtherTalk is used on the Local Mac by opening the Network control panel as shown below:



If EtherTalk is selected, and no zones are displayed, then contact your Distributor or Customer Support.

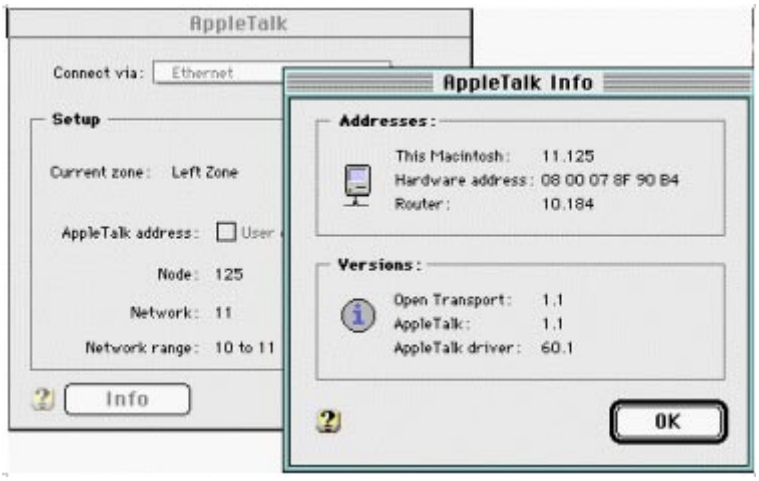
e. If you are using Open Transport, verify that Local Mac has chosen a proper AppleTalk address within the valid network range (this would be 10-11 for the example network) by opening the AppleTalk control panel as shown below:



If the Network Range is correct and the AppleTalk address is not within that range, then try to close the AppleTalk control panel once, and then reopen it. If the AppleTalk address is still invalid, then try to assign a valid address manually by marking *User defined* box. If you start seeing zones, then you can take out the *User defined* tag.

If the Network Range is not correct, contact your Distributor or Customer Support.

f. If the AppleTalk address of Local Mac is valid, then check which AppleTalk router that Local Mac is obtaining the information from by selecting *info* box in the AppleTalk control panel as shown below (this can be done if *Open Transport* is being used):



If the AppleTalk address for the router is not same as the one displayed when issuing `atalk port` console command, then the Local Mac is getting the information from another router. Please refer to the document for the router.

If the AppleTalk address for Router is the same as the one displayed after issuing the `atalk port` console command, contact your Distributor or Customer Support.

4. If only local zones appear and remote zones are not shown in the Mac's Chooser, try the following:

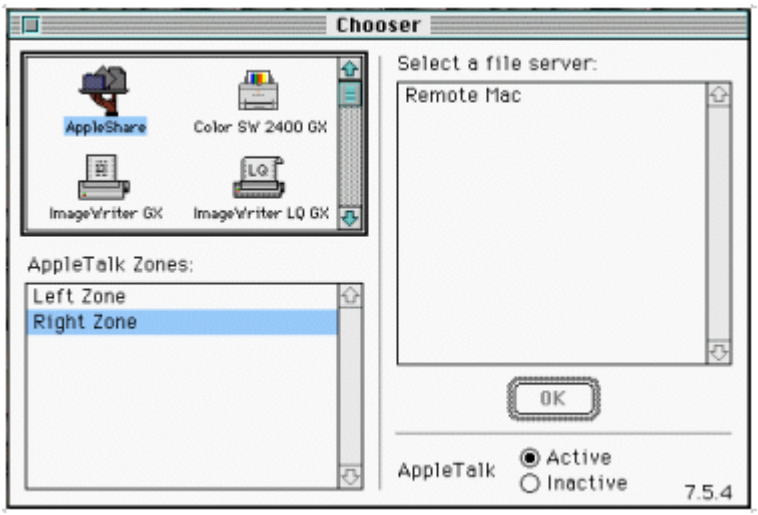
   a. Verify that a static route to the remote network is properly configured on the CyberSWITCH. The static route is configured using CFGEDIT.

   b. If the static route is not configured correctly, make the appropriate corrections.

   c. If the static route is properly configured, then contact your Distributor or Customer Support.

APPLETALK ROUTING OVER A WAN CONNECTION

1. Determine if the Local Mac can access the Remote Mac. On the Local Mac, in the Chooser, pick AppleShare on *Right Zone*:



2. If Remote Mac appears in *Select a file server:* box, then AppleTalk Routing over the WAN connection is operational.

3. If Remote Mac IS NOT displayed, then AppleTalk Routing feature over the WAN connection is not operational, *try the following*:

   a. Verify that AppleTalk Routing is operational on both the local and the remote LAN.

   b. Verify that the remote resources (remote Mac) can be seen when the WAN connection is up.

   c. If the remote resources can be seen when the connection is up but not when the connection is down, there are some problems with making outbound calls. Make sure that the information on the remote CyberSWITCH (labeled *Site 2* in the example network) contains a proper AppleTalk address, and that *Make calls for AppleTalk data* for the device is *enabled*.

   d. If the remote resources can not be seen even when the connection is up, then make sure the AppleTalk address of the remote device is valid. If the remote device is on an unnumbered network, then AppleTalk an address of 0.0 must be configured for the remote device in the device table. If it is on a numbered network, the AppleTalk address does not need to be configured for the device in the device table. However, if it is configured, it must match the AppleTalk address configured on the remote device.

VERIFYING SYSTEM OPTIONS

OVERVIEW

This chapter describes the verification process for various system options. It includes the verification process for:

- *SNMP*
- *Dial Out*
- *Call Detail Recording*
- *Compression*
- *Reserved Bandwidth*
- *DHCP Relay Agent* and *Proxy Client*
- *Semipermanent connections*
- *D Channel Callback*
- *Modem Callback*
- *Proxy ARP*

To perform the verification procedures, WAN lines must be available and ready to use. LAN attachment components must also be available and ready to use.

During some of the procedures, we ask you to enter an administration console command. To enter these commands, you must have an active administration session. If you need instructions for starting an administration session, refer to *Accessing the CyberSWITCH*.

Note: At least one remote device is required to proceed with many of the verification procedures.

SNMP

1. To verify that the SNMP feature is operational, enter the ***snmp stats*** command at the administration console. If the statistics display appears, the SNMP subsystem should be fully operational.

2. If the following message is displayed, SNMP is not operational:

   ```
   SNMP is not enabled
   ```

   Try the following:

   Check the configuration of the CyberSWITCH. In order for the SNMP Agent to become enabled, both the IP option and the SNMP Agent must be enabled in the CyberSWITCH configuration. (You may check the configuration by using the ***options*** and ***snmp*** commands in Manage Mode; however, you can only make changes to these items by using CFGEDIT).

3. Enter the ***dr*** command at the administrative console. If the following message appears, the IP subsystem has initialized successfully:

   ```
   [IP] IP router is initialized successfully
   ```

4. However, if one of the following messages appears, there is an unexpected condition present within the CyberSWITCH software. Contact Customer Support.

   ```
   [SNMP] SNMP initialization failure - unable to allocate
   necessary memory
   [SNMP] SNMP initialization failure - unable to open UDP port
   ```

5. Verify that the MIB objects can be retrieved via the SNMP get command. Begin by making sure that the latest version of the enterprise MIB (the ih_mib.asn file) has been compiled at the desired SNMP network management station(s). Once the new version of the MIB is compiled, you can issue the SNMP get command.

6. Verify the CyberSWITCH SNMP Agent is returning the correct values. Compare the values of the MIB objects retrieved (via the SNMP get command) to the output available via various system administration console and dynamic management commands. For example, the *`isdn usage`* console command displays B-channel information. This information corresponds to the MIB isdnUsageMonitor group objects, a subset of the ihSystemMonitor group. The *`dr`* console command will return output that contains information that corresponds to the MIB ihStatusReport table. Other console commands that will output information that includes values that correspond to MIB objects are *`ds`*, *`udp stats`*, *`ip stats,`* and *`snmp stats.`*

7. Does the CyberSWITCH respond to SNMP requests?

   a. Enter the command *`snmp stats`* at the administrative console. If an "`SNMP is not enabled`" message appears, you must first enable the SNMP Agent (using CFGEDIT).

   b. If the SNMP statistics are displayed, check the value of the "snmpInBadVersions" statistic. If it is non-zero, the Network Management station is generating request PDUs with an incompatible SNMP version number. Such requests are discarded by the SNMP agent.

   c. Check the value of the "snmpInBadCommunityUses" statistic. If it is non-zero, the community name specified in the request PDUs does not have the proper access rights to perform the desired request, and the request is discarded. To correct this problem, reconfigure the MIB access level for the desired community name to the desired access level.

   d. Check the value of the "snmpInASNParseErrs" statistic. If it is non-zero, the network management station is generating request PDUs that are not properly encoded in ASN.1 format. Such requests are discarded by the SNMP agent.

8. Does the CyberSWITCH generate SNMP Trap PDUs?

   a. Enter the *`snmp stats`* command at the administrative console. If an "SNMP is not enabled" message appears, you must first enable the SNMP Agent (using CFGEDIT).

   b. If the SNMP statistics are displayed, check the value of the "`snmpOutTraps`" statistic. If this counter is zero, the SNMP agent has not generated any Traps. Check your configuration setup and ensure that at least one SNMP Trap Receiver is configured. If the value of the "`snmpOutTraps`" statistic is non-zero, the SNMP agent is generating Trap PDUs. If a given Network Management Station is not receiving Traps as expected, check your configuration setup and ensure that the IP address and the Community Name of the Network Management Station that is not receiving Traps is configured properly.

c. Enter *dr* at the administrative console to display the current system messages. If one of the following messages appears, the SNMP agent does not have enough memory to generate all of the Trap PDUs that need to be generated. If the "snmpOutTraps" counter is not increasing while these reports are being logged, there is an unexpected condition present within the CyberSWITCH System software. Contact Customer Support.

```
[SNMP] Unable to obtain an SNMP Trap queue header
[SNMP] Unable to obtain an SNMP Trap queue entry buffer
```

9. Are there authentication problems?
   a. Enter the *dr* console command to display the system log. If the following message is continuously reported in the system log:

```
[SNMP] Authentication failure, unknown community name
```

The Community Name specified in the request PDUs is not recognized by the SNMP Agent. To correct this problem, use CFGEDIT to add the desired community name or change the configuration of your Network Management Station so that it uses a Community Name that is known to the CyberSWITCH.

   b. If the following message is continuously reported in the system log:

```
[SNMP] Authentication failure, improper access rights
```

The Community Name specified in the request PDUs does not have the proper access rights to perform the desired request. Use CFGEDIT to change the MIB access level of the indicated Community Name to the desired access level or change the configuration of your Network Management Station so that it uses a Community Name that has the desired MIB access level.

DIAL OUT

To perform the Dial Out verification for a remote device, you need to know the configured device name associated with the device's device table entry. Note that the device name is case sensitive. If you already know the device name, skip to step 4. Otherwise, begin the verification process with step 1.

1. Enter the Manage Mode by typing the following command at the system prompt:
   >*manage*

2. Enter the following command at the Manage Mode prompt to display the current on-node device table:
   MANAGE> *device*

   Make note of the device name for verification of the Dial Out feature.

3. Exit the Manage Mode by entering the following command:
   MANAGE> *exit*

4. The following administrative command is used to verify that the Dial Out feature is operational to a specific remote device:
   call device <device name>

   For example, to verify that the Dial Out feature is operational for remote device with fred as the configured device name, you would enter *call device fred* at the system prompt.

5. A message will be displayed indicating whether or not the call was made successfully. If the Dial Out call was not completed successfully, *try the following*:

   a. If you issued the *call device <device name>* console command to initiate the call, check to see that you entered the device name correctly. Device names are case sensitive.

   b. If you issued the *call peer <telephone number data rate>* console command to initiate the call, check to see that you entered the correct telephone number and data rate. The telephone number must contain all required prefixes such as the area code, or a "9" if Centrex is used.

   c. If you have entered the call device or the call peer command correctly, follow the *Set Up* and *Action* listed below.

      Set Up:
      - Enable the call trace messages by issuing the *trace on* console command.
      - Erase the current system messages (issue the *er* console command).
      - Initiate a call to a remote device by issuing the *call device <device name>* console command.
      - Display the system messages (issue the *dr* console command).
      - Look for the following call request messages among the system messages.

```
Out - CALL RQST ACK Call Id=<call Id> Rate=<data rate> Slot=<slot#>
   Port=<port#> Chans=<bearer channel map> TN=<telephone number di-
   aled> Ces=<communication endpoint suffix> ConnId=<connect Id
In - CALL RQST ACK CallId=<call Id> Slot=<slot#> Port=<port#>
   CES=<ces> ConnId=<connection Id>
In - PROCEEDING Call Id=<call Id> Slot=<slot #> Port=<port #>
   Chans=<bearer channel map> Ces=<communication endpoint suffix>
   ConnId=< connect Id>
In - CONNECT Call Id=<call Id> Slot=<slot#> Port=<port #>
   Chans=<bearer channel map> Ces=<communication endpoint suffix>
   ConnId=<connect Id>
```

      Action:
      - If the system does not report a call request message for the remote device, then the system did not attempt to make a call. Check to see if there is enough call resources (lines, channels, supported connections) to make the missing call. For example, if your system supports only one BRI line, and you have no hunt groups, then only two active connections are possible. The system would not attempt to make a third call.

        If this is not the case, contact Customer Support.

      - If the system reports a call request message but it does not connect, then the system attempted to make a call. Check to see if the remote device has already completed the installation and verification processes, and is currently running with no active errors.

- If there are no problems, check for the following system messages:

  For BRI resource:
  ```
  In - proceeding <#,#>
  In - disconnect <#,#> - <disconnect cause>
  ```

  For PRI resource:
  ```
  In - accept <#,#>
  In - disconnect <#,#> - <disconnect cause>
  ```

  If the system reports these messages, then the network disconnected the call attempt. For the disconnect cause meaning, refer to the *Cause Code* table. If help is necessary to resolve the reported disconnect cause, write down the "disconnect cause" and call your phone company (carrier) to report the problem.

CALL DETAIL RECORDING

The *cdr verify* console command is used to verify that the Call Detail Recording (CDR) feature is operational. This command will send a sample message to all servers that have been configured for CDR. Check the log file of each server to verify that the message was logged. The message will be similar to the example below; additional data items may be added in future releases.

<System Name> CDR VERIFY 1 of 1

In order for the *cdr verify* console command to be useful, an Ethernet LAN must be operational and an IP route to all off-node servers must be defined and operational. The command can be performed before all the WAN equipment is in place and configured.

Additional verification can be performed by forcing the logged events to occur and checking that they are indeed logged. This would require that all WAN equipment and configuration is in operational order.

The Connect and Disconnect events require a successful connection; a Reject event can be forced by supplying a bad PAP password, for example.

1. Issue the *cdr verify* console command.

2. If the verify fails for an off-node server, *try the following*:

   a. Ping the syslog server to check the IP route from the CyberSWITCH to the server. (Note that an IP route to the server must be established.) If RIP is needed to establish the route, the route may not be available until the CyberSWITCH has been running for a minute or two.)

   b. Using the *dr* command, check the CyberSWITCH Report log for error messages.

   c. Check that the syslogd daemon is running on the syslog server. This can be done with your UNIX system's process status (ps) command. This command should result in a display of the syslogd process. If none is displayed, syslogd is not running.

   d. Syslogd can be run in debug mode with the "*-d*" option. See your UNIX system documentation for more information on your syslogd daemon process.

e. If syslogd is running but does not receive any log messages, make sure CDR is configured for the UDP port that syslogd is using. The typical port is 514, but some versions of syslogd may use a different port.

f. Check that the priority value that you assigned in the CFGEDIT Call Detail Recording menu (default of 38) matches the priority setting on your syslog server (default of auth.info).

COMPRESSION

1. To verify compression is operational, make sure compression is enabled on a system-wide basis.

2. Cause a call to be established with a device for which per-device compression is enabled.

3. To verify that compression is in effect with the device, issue the *cmp stats <devicename>* console command while the connection is in place. If compression is in effect, this command will display the current compression counters and ratios.

4. If compression is not in effect, the command will return an indication that the device is a non-compressed connection. If compression is not in effect, *try the following*:

   a. Issue the *cmp stats* console command then issue the *dr* console command to check the message report log. A message will inform you if the compression failed due to memory constraints.

   b. Verify that the CyberSWITCH has compression enabled. This is done through selecting "Compression Options" from CFGEDIT's Systems Options menu.

   c. Verify that the device to which the connection is being established has compression enabled. If the device is another CyberSWITCH, refer to the previous step for instructions.

   d. Use the trace console command to examine the CCP frames exchanged with the device. This is typically accomplished by issuing the *trace ppp on* command, erasing the log contents, establishing the call, and then examining the log again (by issuing the *dr* console command) to view the frame trace.

      The following traces illustrate some common PPP start-up scenarios when compression is enabled. Only the CCP frames are excerpted for clarity.

   - Successful Negotiation
     As a reference, the following trace illustrates a successful negotiation of CCP using the Stac compression protocol. The key feature of this sequence is that each side receives a CONFIG-ACK to its respective CONFIG-REQ.

```
(I) 15:35:09.98 #80FD: Conn=001 OUT-PPP:CCP      CFG REQ Id=0xB4 Len=9
(I) 15:35:09.98 #9999: -Alg: 0x11 (STAC-LZS) Len: 5
(I) 15:35:09.98 #9999:   Hist Count: 01   Chk Mode: 0x03 (SEQ#)
(I) 15:35:09.98 #80FD: Conn=001 IN -PPP:CCP      CFG REQ Id=0x7B Len=9
(I) 15:35:09.98 #9999: -Alg: 0x11 (STAC-LZS) Len: 5
(I) 15:35:09.98 #9999:   Hist Count: 01   Chk Mode: 0x03 (SEQ#)
(I) 15:35:09.99 #80FD: Conn=001 OUT-PPP:CCP      CFG ACK Id=0x7B Len=9
(I) 15:35:09.99 #9999: -Alg: 0x11 (STAC-LZS) Len: 5
(I) 15:35:09.99 #9999:   Hist Count: 01   Chk Mode: 0x03 (SEQ#)
(I) 15:35:09.99 #80FD: Conn=001 IN -PPP:CCP      CFG ACK Id=0xB4 Len=9
(I) 15:35:09.99 #9999: -Alg: 0x11 (STAC-LZS) Len: 5
(I) 15:35:09.99 #9999:   Hist Count: 01   Chk Mode: 0x03 (SEQ#)
```

- *Peer Protocol-Rejects CCP*
  If the peer does not actually support PPP compression, it will most likely Protocol-Reject the CyberSWITCH's attempt to negotiate CCP. In this case, the CyberSWITCH will abandon its attempt to use compression and the connection will operate uncompressed. The incoming frame from the peer contains a PROT-REJ, whose 1st two hex octets in the trace indicate the CCP protocol (0x80FD).

```
(I) 16:01:51.65 #80FD: Conn=001 OUT-PPP:CCP      CFG REQ Id=0x87 Len=9
(I) 16:01:51.65 #9999: -Alg: 0x11 (STAC-LZS) Len: 5
(I) 16:01:51.65 #9999:   Hist Count: 01   Chk Mode: 0x03 (SEQ#)
(I) 16:01:51.65 #C021: Conn=001 IN -PPP:LCP      PROT REJ Id=0x00 Len=15
(I) 16:01:51.71 #0000:   80 FD 01 87 00 09 11 05 00 01 03
```

- *The CyberSWITCH does not have Compression ENABLED*
  In this case, the CyberSWITCH will respond to all attempts by the peer to open CCP with a TERM-ACK frame. The connection will operate uncompressed. (Note: a device that supports compression but has it disabled will typically do the exact same thing).

```
(I) 15:36:40.54 #80FD: Conn=001 IN -PPP:CCP      CFG REQ Id=0xEC Len=9
(I) 15:36:40.54 #9999: -Alg: 0x11 (STAC-LZS) Len: 5
(I) 15:36:40.54 #9999:   Hist Count: 01   Chk Mode: 0x03 (SEQ#)
(I) 15:36:40.54 #80FD: Conn=001 OUT-PPP:CCP      TERM ACK Id=0xEC Len=4
```

RESERVED BANDWIDTH

1. To verify bandwidth reservation, configure several different combinations of lines and devices.
2. Attempt outbound and inbound calls.
3. Verify the proper success and reject of each.
4. If there is a problem, check the configuration of the profiles and how they are assigned to each device (refer to *Bandwidth Reservation* in the *Configuring Call Control* chapter).

DHCP RELAY AGENT

The following sections provide instructions to verify that the DHCP/BOOTP Relay Agent is working properly.

VERIFYING DHCP RELAY AGENT INITIALIZATION

Regardless of whether or not the Relay Agent has been enabled via configuration, some initialization processing is always performed. If this initialization is successful, there should not be any warnings/errors written to the report log by the DHCP Relay Agent.

1. Examine the report log. Type:
   dr <return>

2. The *dr* command displays the system report log. Look for any messages that begin with:
   `[DHCP-R]`

3. The following messages indicate that errors occurred during DHCP/BOOTP Relay Agent initialization processing:
   ```
   [DHCP-R] Failed to allocated memory for transmit buffer pool
   [DHCP-R] Relay Agent initialization failed
   ```

   If you do not see either of these messages in the report log, the DHCP/BOOTP Relay Agent has successfully performed its initialization processing.

4. If either (or both) of the above messages are contained in the report log, try the following:

   Look for the following messages after system initialization:
   ```
   [DHCP-R] Failed to allocated memory for transmit buffer pool
   [DHCP-R] Relay Agent initialization failed
   ```

   These messages indicate that an error occurred during initialization of the DHCP/BOOTP Relay Agent. Therefore, the relay agent will not operate correctly. Contact your Distributor or Customer Support.

VERIFYING THE RELAY AGENT IS ENABLED

If the Relay Agent has been enabled via configuration, it will attempt to open a UDP port for use. A message describing the outcome of this operation will appear in the report log.

1. Examine the report log. Type:
   dr <return>

2. Look for any messages that begin with [DHCP-R].

3. If the Relay Agent has been enabled via configuration, the following message should appear:
   ```
   [DHCP-R] Relay Agent enabled; UDP port (67) opened
   ```

   If the above message was found in the report log, the Relay Agent has been successfully enabled.

4. If an error occurred while trying to enable the Relay Agent, the following message may be displayed in the report log:

   ```
   [DHCP-R] Failed to open UDP port (67), erc=<error return code>
   ```

   This indicates that an internal error occurred while trying to open a UDP port for use by the DHCP/BOOTP Relay Agent. Therefore, the relay agent will not operate correctly. Contact your Distributor or Customer Support.

5. If the following message is NOT found in the report log after system initialization:

   ```
   [DHCP-R] Relay Agent enabled; UDP port (67) opened
   ```

   It indicates that there was no attempt made to enable the DHCP/BOOTP Relay Agent. *Try the following*:

   a. Check the DHCP configuration. This can be done by using CFGEDIT, or by using the *dhcp* command from Manage Mode.

   b. Make sure that the Relay Agent is enabled.

   c. If desired, enter MANAGE mode, and use the *dhcp change* command to enable the Relay Agent. (Note: CFGEDIT can also be used to change the Relay Agent configuration; but the changes will not take effect until the system is restarted.)

   d. When Manage Mode is exited, an attempt will be made to enable the Relay Agent.

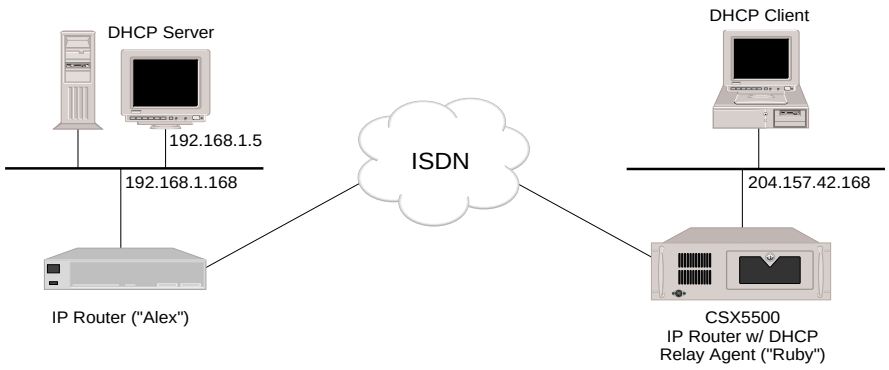
   e. Re-examine the report log for the "Relay Agent Enabled" message.

   f. Remember to "commit" the Manage Mode configuration changes to make them permanent.

VERIFYING THE RELAY AGENT IS OPERATIONAL

Once the Relay Agent has been successfully initialized and enabled, DHCP Clients should be able to obtain their IP addresses (and other configuration parameters) from a DHCP Server.

For example purposes, assume the following diagram represents the network in which the Relay Agent is being used. This configuration is useful when a remote IP router is known to have access to a DHCP Server, but that router is not a DHCP/BOOTP Relay Agent.



In this configuration, the DHCP Client is able to obtain its IP address from the DHCP Server, using the Relay Agent contained in the IP Router on the client's LAN ("Ruby").

Shortly after a DHCP Client is powered on, it will attempt to get its IP address from a DHCP Server. If it is successful, its IP-related features (e.g., ping, telnet, etc.) will become operational. If the client could not obtain its IP address, it will retry periodically to do so.

1. From the DHCP Client, attempt to ping the Relay Agent ("Ruby") that is on the same LAN:

```
C:\> ping 204.157.42.168 <return>

Pinging 204.157.42.168 with 32 bytes of data:
Reply from 204.157.42.168: bytes=32 time=2ms TTL=64
Reply from 204.157.42.168: bytes=32 time=2ms TTL=64
Reply from 204.157.42.168: bytes=32 time=1ms TTL=64
Reply from 204.157.42.168: bytes=32 time=2ms TTL=64
```

   A response of this form indicates that the IP-related features of this client are enabled. Therefore, it has successfully obtained an IP address from the DHCP Server.

2. If the ping attempt resulted in something like the following, the client was not able to obtain its IP address from the DHCP Server:

```
C:\> ping 204.157.42.168

Pinging 204.157.42.168 with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
```

   If this is the case, *try the following*:

   a. Check the DHCP configuration. This can be done by using CFGEDIT, or by using the *dhcp* Manage Mode command.
   b. Make sure that the Relay Agent is enabled on the desired machine. Check the report log. A message is written to it by the DHCP Relay Agent when it has been successfully enabled.
   c. Make sure that the DHCP Relay Agent is properly configured. There must be a relay destination configured for the desired DHCP Server, or for the next DHCP Relay Agent to go through.
   d. If the machine being configured is an intermediate DHCP Relay Agent, make sure that the Hop Threshold is large enough to allow the number of Relay Agent "hops" between the DHCP Client and the DHCP Server.
   e. From the DHCP Server, you should be able to "ping" the DHCP Relay Agent closest to the DHCP Client. If you cannot, you need to add static routes that allow you to do so.
   f. From the DHCP Relay Agent closest to the DHCP Client, you should be able to "ping" the DHCP Server. If you cannot, you need to add static routes that allow you to do so.
   g. The DHCP Server must be configured to distribute addresses to clients on the DHCP Client's subnetwork.

DHCP: PROXY CLIENT

The following sections provide instructions to verify that the DHCP Proxy Client is working properly.

VERIFYING DHCP PROXY CLIENT INITIALIZATION

Regardless of whether or not the Proxy Client has been enabled via configuration, some initialization processing is always performed. If this initialization is successful, there should not be any warnings/errors written to the report log by the DHCP Proxy Client.

1. Examine the report log. Type:
   dr <return>

2. The *dr* command displays the system report log. Look for any messages that begin with:
   `[DHCP-P]`

3. The following message indicate that errors occurred during DHCP Proxy Client initialization processing:
   `[DHCP-P] Proxy Client initialization failed`

   If you do NOT see this message in the report log, the DHCP Proxy Client has successfully performed its initialization processing.

4. If you DO receive an *initialization failed* message, the DHCP Proxy Client will not operate correctly. Contact your Distributor or Customer Support.

VERIFYING THE PROXY CLIENT IS ENABLED

If Proxy Client has been enabled via configuration, a relevant message will appear in the report log:

1. Examine the report log. Type:
   dr <return>

2. Look for any messages that begin with [DHCP-P].

3. If the Proxy Client has been enabled via configuration, the following message should appear:
   `[DHCP-P] Proxy Client enabled`

   If the above message was found in the report log, the Proxy Client has been successfully enabled.

4. If the message is NOT found in the report log after system initialization, *try the following*:

   a. Check the DHCP configuration. This can be done by using CFGEDIT, or by using the *dhcp* command from Manage Mode.

   b. Make sure that the Proxy Client is enabled.

c. If desired, enter MANAGE mode, and use the *dhcp change* command to enable the Proxy Client. (Note: CFGEDIT can also be used to change the Proxy Client configuration; but the changes will not take effect until the system is restarted.)

d. When Manage Mode is exited, an attempt will be made to enable the Proxy Client.

e. Re-examine the report log for the "Proxy Client Enabled" message.

f. Remember to "commit" the Manage Mode configuration changes to make them permanent.

5. If an error occurred while trying to enable the Proxy Client, the following message may be present in the report log:

```
[DHCP-P] Failed to register with the IP Address Pool Manager,
erc=<error code>
```

If this error message is found in the report log, it indicates that an internal error occurred while the DHCP Proxy Client was trying to register as a provider of addresses for the IP Address Pool. Therefore, the proxy client will not operate correctly. Contact your Distributor or Customer Support.

VERIFYING THE PROXY CLIENT IS OPERATIONAL

Once the DHCP Proxy Client manager has been successfully initialized and enabled, it should begin obtaining IP addresses from DHCP servers. The manager examines any WAN and WAN (Direct Host) network interfaces. It then attempts to satisfy the "number of IP addresses to pre-fetch" for each of these network interfaces.

VERIFICATION OF UDP PORTS

In order to reach DHCP servers, the DHCP Proxy Client will open the BOOTPC UDP port, and possibly the BOOTPS UDP port. One or both of the following messages should then appear in the report log:

```
[DHCP-P] UDP port (67) opened
[DHCP-P] UDP port (68) opened
```

If neither of these messages is found in the report log, *try the following*:

a. Check the DHCP-related configuration for WAN and WAN (Direct Host) IP network interfaces which should have IP addresses obtained from DHCP servers for them. Use CFGEDIT, or use the *ipnetif* command from Manage Mode. Correct if necessary.

b. Make sure that the *maximum addresses to obtain* for the interface is non-zero.

c. Make sure that the *number of addresses to pre-fetch* for the interface is non-zero.

d. The DHCP Server must be configured to distribute addresses to clients on the DHCP Client's subnetwork.

VERIFICATION OF IP ADDRESS POOL

As IP addresses are obtained from DHCP servers, they are placed into the system's IP Address Pool. To verify the presence of these DHCP-obtained IP addresses, perform the following:

1. Examine the address pool. Type:
   `ip addrpool` <return>

2. Look for addresses with an origin of DHCP. This verifies that IP addresses were obtained from a DHCP server, and the Proxy Client is working correctly.

3. If no "DHCP-obtained" addresses are present in the IP Address Pool, *try the following*:
   a. Check the DHCP-related configuration for WAN and WAN (Direct Host) IP network interfaces which should have IP addresses obtained from DHCP servers for them. Use CFGEDIT, or use the `ipnetif` command from Manage Mode. Correct if necessary.

   b. Make sure that the *LAN port to reach the DHCP server on* for the interface is correct.

   c. If the DHCP server is on a directly-connected LAN, you should be able to `ping` it successfully from the CyberSWITCH. If you cannot, check the LAN port IP configuration; make sure the DHCP server is operational.

   d. If the DHCP server is not on the directly-connected LAN, a DHCP Relay Agent must be. A relay agent is required in order to successfully forward DHCP packets to a DHCP server on a different sub-network.

   e. Assuming that a DHCP Relay Agent is present on the directly-connected LAN, you can attempt to `ping` the DHCP server. This may require the addition of IP static routes on both the CyberSWITCH and the DHCP server. These static routes are required for smooth operation of the DHCP protocol.

   f. If the DHCP server is not on a directly-connected LAN, another test may be performed. If at all feasible, place a DHCP client workstation on the same LAN with the server. See if this DHCP client can obtain an IP address from the DHCP server.

D CHANNEL CALLBACK

1. On the CyberSWITCH:

   a. Make sure you are using the Connection Services Manager (CSM) for device authentication.

   b. Make sure you have enabled D Channel callback.

2. Define the calling devices on CSM. For each calling device configured through CSM, make sure you:

   a. Configure the device as an ISDN connection (under the device's *Telephone* tab).

   b. Configure the telephone number to be used to call back to the calling device (under the device's *Telephone* tab).

c. Configure a calling line ID for the number the device will be using when calling into the CyberSWITCH (under the device's *Telephone* tab).

d. Enable callback (under the device's *Access/Other* tab).

e. Enable outbound authentication if you want to make sure the device you are calling back to is the correct device (under the device's *Access/Authentication* tab).

3. On the CyberSWITCH:

a. Enable the call trace message option by issuing the `trace on` console command.

b. Erase the current system messages (issue the `er` console command).

c. Initiate a call from the remote device to the CyberSWITCH.

d. Display the system messages (issue the `dr` console command). You should see the incoming call and possibly some proceeding / alerting messages, then a disconnect. In approximately 10 seconds, you should see an outgoing call to the remote site and a connect message.

4. If the initial call completes but never does a drop and callback check for the following:

a. Make sure D Channel callback is enabled on the CyberSWITCH.

b. Make sure the device is configured for callback through CSM.

c. Make sure the correct CLID was entered for the device through CSM.

d. Investigate to make sure a CLID was presented.

MODEM CALLBACK

1. On the CyberSWITCH, make sure you are using CSM for device authentication.

2. Define the calling devices on CSM. For each calling device configured through CSM, make sure you:

a. Configure the device as a modem connection (under the device's *Telephone* tab).

b. Configure the telephone number to be used to call back to the calling device (under the device's *Telephone* tab).

c. Configure a calling line ID for the number the device will be using when calling into the CyberSWITCH (under the device's *Telephone* tab).

d. Enable callback (under the device's *Access/Other* tab).

e. Enable outbound authentication if you want to make sure the device you are calling back to is the correct device (under the device's *Access/Authentication* tab).

3. On the CyberSWITCH:

   a. Enable the call trace message option by issuing the `trace on` console command.

   b. Erase the current system messages (issue the `er` console command).

   c. Initiate a call from the remote device to the CyberSWITCH.

   d. The remote device should indicate it is waiting for a callback.

   e. Display the system messages (issue the `dr` console command). You should see the incoming call and possibly some proceeding / alerting messages, a connect, then a disconnect. In approximately 300 seconds, you should see an outgoing call to the remote site and a connect message.

   f. The remote device should answer the incoming call and connect.

4. If the modem answers but n o pop up screen comes up to prompt for a callback number, make sure the callback checkbox is checked for this device through CSM.

5. If you enter the phone number in the callback pop up but no call back ever occurs, check the following:

   a. Make sure you entered the correct number in the callback pop up.

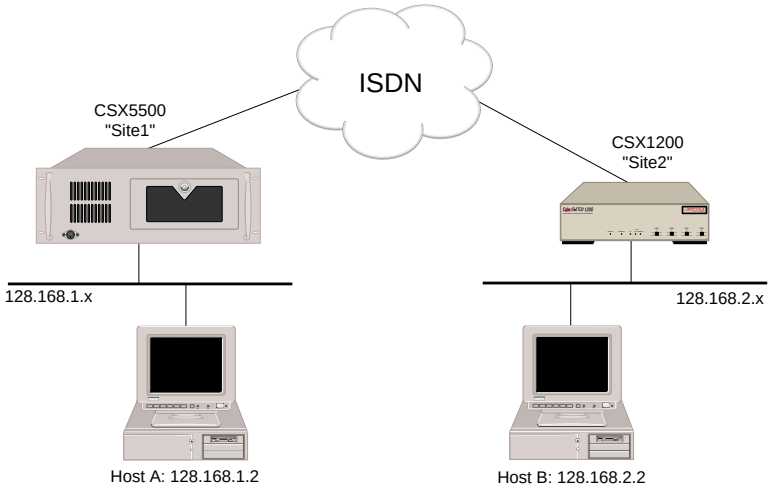
   b. Check to see if the phone number entered needs a Centrex digit (a 9 before the phone number).

VERIFYING A SEMIPERMANENT CONNECTION

Follow the same procedure outlined in the *Dial Out* section. If you can successfully use the call device command to call the device assigned to the semipermanent connection, then the connection is working. If not, follow the instructions actions in the dial out verification section.

PROXY ARP

Use the following graphic to help you in verifying that Proxy ARP is operational. When following the verification steps, substitute your addresses for the addresses used in the example.



1. Create two Ethernet LANs connected across the WAN with a CyberSWITCH and a second Cabletron platform (for example, another CyberSWITCH product) properly configured. The two Ethernet segments should be subnets of the same IP network. All IP host devices on the Ethernet segments (except the CyberSWITCH and the other Cabletron platform) should be configured with the natural subnet mask so that both Ethernet segments look like one IP network to all the IP host devices on the segments.

2. Try to have an IP host device on one Ethernet segment communicate with an IP host device on the other Ethernet segment. For example, ping from Host A to Host B.

3. If the communication between two IP devices across the WAN is successfully established, then the proxy ARP feature is properly working.

4. If the communication can NOT be established, display the ARP cache on the IP host devices to see what MAC addresses are mapped to the target IP address. On many operating systems, the *`arp -a`* command displays the ARP cache. If the target IP addresses are mapped into the nearest CyberSWITCH's MAC addresses respectively, for example, on Host A, Host B's IP address is mapped to the CyberSWITCH A's MAC address, then the proxy ARP feature is working properly, but basic IP routing may not be operational. Establish the basic IP connectivity first, then try to use the proxy ARP feature. If the target IP addresses are not shown (or are mapped to MAC addresses that are not displayed), *try the following*:

   a. On both CyberSWITCH platforms, issue the *`ipnetif`* manage mode command to make sure that the proxy ARP feature is enabled for the LAN interface. If it is not enabled on one or both of the CyberSWITCH platforms, enable it through the CFGEDIT configuration utility. Note that you have to restart the system for the changes to be effective.

   b. On both platforms, issue the *`ipnetif`* manage mode command to make sure the LAN interfaces are configured with the proper subnet mask. Configure these platforms with the proper subnet masks, not the natural masks.

c. On both platforms, issue the *iproute* manage mode command to make sure that each system knows about the IP subnet at the other Ethernet segment.

d. If the two IP host devices still can not communicate with each other, contact your Distributor or Customer Support.

TROUBLESHOOTING

We include the following chapters in the *Troubleshooting* segment of the *User's Guide*:

- *LCD Messages*
  Provides an explanation of the LCD messages. These messages can provide valuable information for troubleshooting.

- *System Messages*
  Provides a listing of all system messages, their meanings, and when applicable, possible actions you should take.

- *Trace Messages*
  For certain features you may turn a trace option on, allowing you to track system messages particular to that feature. Information is included describing how to turn the trace options on. We also list possible resulting trace messages and their meanings. The trace option is available for the following features: call trace, frame relay (LAPB), PPP packets, and X.25.

  Also refer to the *Verification and Diagnosis* segment which provides scenarios in which these messages may occur.

LCD MESSAGES

OVERVIEW

The CyberSWITCH has an LCD display on its front panel, which displays information in a two-line format. The first line displays initialization and current status information (which includes any errors that have been detected). The second line displays current connection information. These messages can also be displayed on the monitor by issuing the *status* command.

LCD MESSAGE GROUPS

There are three groups of LCD messages: initialization, normal operation, and error messages.

INITIALIZATION LCD MESSAGE

```
Initializing...
```

Appears on the LCD display during system initialization.

NORMAL OPERATION LCD MESSAGES

During normal operation, the system tracks / displays connectivity information. This includes how many sites (xx) the system is currently connected to, each site that is currently connected, and the amount of bandwidth (xxx) in use.

```
Calls Active
xx Active Sites
```

Current number of Sites connected.

```
Calls Active
xxx to <sitename>
```

Bandwidth to each site.

```
No Sites Connected
```

No sites connected.

```
No Active Calls
0 Active Sites
```

No sites connected.

ERROR LCD MESSAGES

The system keeps track of all active errors and displays / records them in a cycle. When the system detects an error, it displays the error on the first line of the LCD. (The "s" indicates slot, "p" indicates port, and "c" indicates bearer channel.) The LCD will continue to display the current connection information on the second line.

To further investigate an error LCD message, enter the *dr* command at the console. Take the appropriate corrective actions related to the displayed system messages.

```
(s,p) Cfg Error
```

Line vs. adapter configuration error. A line is configured for port "p" that does not exist on the adapter in slot "s".

```
Ded (s,p,c) Down
```

Dedicated Connection failure. The Dedicated Connection on the line connected to slot "s", port "p", starting at starting bearer channel "c" is down.

```
X25PVC (access, PVC) Down
```

X.25 Permanent Virtual Circuit (PVC) failure for the indicated PVC.
Where:

access = access index
PVC = permanent virtual circuit index

```
DL (s,p,ces) Down
```

The specified data link for a line is down.

```
File Access Err
```

System unable to access file. Check for one of the following log error messages:

```
Error opening file <file name>
Error reading file <file name>, section = <section name>
Error opening file <file name>, slot <slot #>
Read 0 bytes from file <file name> for WAN card in slot <slot #>
Failure during read of file <file name> for WAN card in slot <slot #>
Error closing file <file name>, slot <slot #>
Error closing password data file
Error opening password data file
Failure on closure of file <file name>
Failure opening file <file name>
Failure on file closure <file name>
Failure on write of file <file name>
```

If you see any of the above log messages repeatedly, there may be a problem with your hard drive. Contact your Distributor or Customer Support.

```
LAN HW Error
```

LAN connection failure. Hardware failure detected on the Ethernet LAN adapter. Check for one of the following log error messages:

```
Manual intervention required: please replace LAN card
Lan Adapter HW upgrade required
Lan Adapter HW upgrade may be required
```

With any of the above messages, refer to the *System Messages* chapter for specific error message resolution.

```
LAN Init Error
```

LAN connection failure. Initialization failure detected by the LAN packet forwarding component in the system.

```
LAN Xmit Error
```

LAN connection failure. LAN packet transmit error detected by the system.

```
Line (s,p) Down
```

ISDN line failure. The data link for the line connected to slot “s” port “p” is down.

```
Out Svc # (s,p)
```

ISDN line failure. The line connected to slot "s" port "p" is out of service for the reason indicated by #.

1 = No layer 1 sync for 5 seconds
This problem normally occurs due to WAN cabling problems.
Check your cables to make sure they are connected correctly. If the problem still occurs after you have checked all the cables, call the phone company and report the problem.

2 = No response to TEI requests
This problem normally occurs due to invalid configuration.
Check your configuration using the following table:

basic rate only	line from phone company: point-to-point	line from phone company multi-point (Japan only)
line configured on system: non-auto TEI	make sure that the configured system TEI value is 0	change TEI to be AUTO
line configured on system: auto TEI	change system TEI to be non-auto	if problem happens for over 5 minutes, report problem to phone company

3 = No UA response to SABME requests; no Layer 2
This problem normally occurs due to invalid configuration.
Check your configuration using the following table:

basic rate and primary rate	line from phone co: point-to-point	line from phone co: multi-point (Japan only)
line configured on system: non-auto TEI	make sure that the configured TEI value is 0	change TEI to be AUTO
line configured on system: auto TEI	change TEI to be non-auto	if problem happens for over 5 minutes, report problem to phone company

4 = Network sent CAUSE - invalid SPID
This problem normally occurs due to an invalid SPID configuration.
Enter the correct SPID for the line. If you think that the correct SPID has been entered, contact your phone company.

5 = Network sent init, but no SPID configured
This problem normally occurs because the SPID was not configured. Configure the correct SPID for the line.

```
Over Max Charge
```

Monthly call charges exceeded. Monthly call charge tracking is enabled and the configured maximum has been exceeded.

```
Semiperm Error
```

There is an problem with the semipermanent connection. A more detailed error message is displayed in the log messages. Display the log messages (enter *dr* command) and look for “Semipermanent.....” messages.

SYSTEM MESSAGES

OVERVIEW

System Messages provide useful system information. They are listed in the system's report log, a memory resident table. To manipulate the report log, use the following commands at the administrative console:

dr or *ds*	display reports or display statistics
er or *es*	erase current messages / statistics from memory
wr or *ws*	write reports / statistics to disk

When the CyberSWITCH writes system messages to disk, it stores them in the following locations:

Directory:	`\log`
File Name:	`rprt_log.nn` (where "nn" is an integer from 1 to 10 that is incremented each time a new file is written.)

The system reports messages using the following format:

Message Type	Time	Report Number	Message
I Informational W Warning E Error	hour:minutes:second	internal ID for area reporting the message	actual text of the message

- the Message Type quickly identifies the type of message the system reports
- the Time identifies when the message was reported
- the Report Number is used by your Distributor or Customer Support
- the Message text describes the actual message being reported

This chapter describes the types of system messages available (for example, informational and error). It also lists each message individually, with suggested actions to take in the event of an error.

Notes: In addition to the system report log, there are separate logs for both *call detail recording* and *authentication messages*. Prior to software release 7.3, the authentication messages were included in the system report log. With release 7.3, these authentication messages now appear in a separate log. You may access this authentication log with the commands:

da	to display authentication messages
ea	to erase current authentication messages
wa	to write authentication messages to disk

The authentication messages are still described within this chapter. For descriptions of possible call detail recording messages, refer to *Event Report Contents* in the *Advanced Options* chapter.

Also note that some system options require you to enable a trace before messages concerning these options are recorded in the system report log. Refer to the *Trace Messages* chapter for more information.

INFORMATIONAL MESSAGES

The system records informational messages. These are normal events that provide you with current system status. Informational messages include the following categories of messages:

- initialization messages
- normal operation messages
- Spanning Tree messages

INITIALIZATION MESSAGES

The system reports a variety of messages during a successful system initialization. These messages may include: status of bridge, status of LAN ports and adapters, data link, SNMP, and TFTP information. The following are examples of typical initialization messages:

```
Bridge is operating in UNRESTRICTED mode
Data link up: Slot=<slot #> Port=<port #> Ces=<comm. endpoint suffix>
[SNMP] SNMP initialized successfully
```

NORMAL OPERATION MESSAGES

The system normal operation messages may include information such as:

```
Call Restrictions have been disabled by user command
WAN Port is now in the <new state> state
```

SPANNING TREE MESSAGES

The Spanning Tree protocol is only supported by the Ethernet-2 interface card.
Spanning Tree protocol messages are prefaced with [STP]. During normal operation, when Spanning Tree protocol is enabled, the system may report informational messages such as:

```
[STP] A new Root Bridge has been detected
[STP] LAN Port <port #> is now a Designated Port
```

WARNING MESSAGES

System warning messages signal events that you should investigate. These messages may be normal during certain network conditions, or they may indicate a problem. The system should continue to operate after posting a warning message. If the system fails to operate normally, then report it using the problem report form included in *Getting Assistance.*

ERROR MESSAGES

When the system detects errors, it reports error messages. If the faulty component cannot be identified, and an error condition persists, then report the error by using the problem report form included in *Getting Assistance*.

SYSTEM MESSAGE SUMMARY

The following pages list all the informational, warning and error messages alphabetically. The text describes the messages, and includes suggestions for problem resolution (if applicable). Note that the trace messages have been isolated for your convenience, and are summarized in the next chapter.

<timestamp> #000: Couldn't open the file C:\SYSTEM\PLATFORM.NEI
The open operation failed, no further detail is available.

<timestamp> #0000: Error reading C:\SYSTEM\PLATFORM.NEI
The read operation failed, perform a software upgrade to reinstall the file.

<timestamp> #0000: Error reading platform type: there is no "plat name" field
There is no <platform name> value following the "=" character in the "current setting" string.

<timestamp> #0000: Error reading platform type: there was no "=" in the string
The "current setting" string has the format "<platform type>=<string>". This error message indicates that no "=" character exists in the string.

<timestamp> #0000: Error reading platform type: type value is too large
The <platform type> value in the "current setting" string is too large to represent an actual platform type.

<timestamp> #0000: Error reading platform type: type was not converted to an int
The <platform type> value in the "current setting" string could not be converted to an actual platform type.

1 port LAN Adapter, operating in remote mode only
This is an initialization message. It identifies the Ethernet adapter type (Ethernet-1), and operating mode. Remote bridging is supported.

2 port LAN Adapter, operating in local and remote mode
This is an initialization message. It identifies the Ethernet adapter type (Ethernet-2), and operating mode. Both local and remote bridging are supported.

aarp found duplicate AppleTalk address <AppleTalk Address> @ <MAC address>
The address resolution protocol found duplicate AppleTalk addresses for this AppleTalk network. Check the configuration for the AppleTalk ports' network range / number.

Abnormal response rcvd: <state msg reason cc state>
An unexpected message was received from a WAN interface card. The <parameters> included are for problem reporting purposes only. If the system fails to operate normally, or the warning continues to occur, contact your Distributor or Customer Support.

A call has exceeded the configured maximum duration
A call has been up longer than the amount of time configured. The next log message will inform the user whether or not the call has been taken down.

[ACCT] Warning code: Timeout
This message is logged when there is no communication with the server. Either the accounting server is not up and running, or it cannot access the IP address. Verify the configuration of the server.

ACE authentication is not available. You must first ENABLE ACE user level authentication.
An attempt was made to configure the Terminal Server Security for ACE and ACE was not configured on the CyberSWITCH.

Activation Failure- Session NOT active
An error has been detected in the R2 signaling procedure, and will typically result in a failed call. The error was due to unrecognizable or incorrect information. If problem persists, contact your Distributor or Customer Support.

Adapter does not respond: adapter #'x'
The WAN card initialization subsystem encountered an error on the indicated adapter. Restart the system. If the problem persists, the indicated adapter card may be faulty and you should contact your Distributor or Customer Support.

Adapter #'x' failed to initialize
The operational software on the indicated adapter card failed to signal that initialization was completed. Restart the system. If the problem persists, the indicated adapter card may be faulty and you should contact your Distributor or Customer Support.

Adapter #'x' failed to respond from bootstrap
The WAN card initialization subsystem encountered an error on the indicated adapter while downloading the bootstrap program. Restart the system. If the problem persists, the indicated adapter card may be faulty and you should contact your Distributor or Customer Support.

Adapter failed to respond while programming: adapter 'x'
The WAN card initialization subsystem encountered an error on the indicated adapter while programming the hardware. Restart the system. If the problem persists, the indicated adapter card may be faulty and you should contact your Distributor or Customer Support.

Administrative Session using ACE does not support password change.
Passwords may only be changed via the ACE Server administrator initiation. During an administrative login, the user attempted to change password. ACE only supports password change initiated by ACE Server administrator.

AppleTalk routing initialized successfully.
This message is posted when the system AppleTalk routing feature has initialized successfully.

AppleTalk routing RTMP initialization error, AppleTalk disabled
AppleTalk is disabled because there is an initialization problem with the Routing Table Maintenance Protocol (RTMP). Contact your distributor or Customer Support.

AppleTalk routing ZIP initialization error, AppleTalk disabled
AppleTalk is disabled because there is an initialization problem with the Zone Information Protocol (ZIP). Contact your distributor or Customer Support.

AppleTalk successfully initialized on LAN port <port number> with address <AppleTalk address>.
This message is posted when the specified AppleTalk LAN port has initialized successfully.

AppleTalk successfully initialized on WAN port with address <AppleTalk address>.
This message is posted when the specified AppleTalk WAN port has initialized successfully.

Attempted to start timer for inactive Signaling Session.
Attempted to stop timer for inactive Signaling Session.
Attempted to use session with no event handler.
An error has been detected in the R2 signaling procedure, and will typically result in a failed call. The error was due to unrecognizable or incorrect information. If problem persists, contact your Distributor or Customer Support.

Attempting to Autobaud, Press <CR> Many Times, Quickly
The user has requested that the RS 232 port undergo an autobaud procedure, or the RS232 port has not been properly Autobauded.

Attempting to load "<FileName>" for Upgrade
A Reliable Remote Upgrade has taken place. The specified file is now being loaded into memory for verification and subsequent installation into the Flash File System.

Attempt to reinitialize DM card in slot <slot #>
The system is attempting to initialize the Digital Modem card again after a failed attempt. Check the subsequent log messages for the status of the card.

Attempt to initialize unconfigured DM card in slot <slot #>
The system is attempting to initialize a Digital Modem card, with no success. This is likely a configuration problem. Check CFGEDIT setup to ensure that it correctly matches existing hardware.

[AUTH] ACE Client has not been initialized.
The ACE client has not been initialized. No service file exists. Server should be expecting CyberSWITCH client to request node verification. Contact the ACE administrator and request the client to be reinitialized.

[AUTH] ACE Could not create service file.
The CyberSWITCH ACE client was in an initialized state. After receiving service information from the ACE server a local file create error occurred while attempting to save the information.

[AUTH] ACE Could not synchronize client-server.
During an authentication attempt the client was unable to synchronize with the server and the user was rejected. The server may not be responding to the client.

[AUTH] ACE Could not write service file.
The CyberSWITCH ACE client was in an initialized state. After receiving service information from the ACE server a local file write error occurred while attempting to save the information.

[AUTH] ACE Decryption of server response failed.
Sever response to an ACE client request was received, but could not be decrypted. Verify encryption method configured for server is accurate.

[AUTH] ACE Encryption configured for DES: not supported.
The ACE server is configured for DES encryption. Only SDI encryption is currently supported by the ACE client.

[AUTH] ACE Error receiving server log message acknowledgment.
A client syntax error occurred during an authentication attempt via ACE. The server did not respond to the logging of the message. Make sure the ACE server configuration is accurate.

[AUTH] ACE LOGIN rejected user: <user name>
The remote Authentication server rejected the named user. This indicates that one of the following has occurred:

1. The <user name> is not in the remote Authentication server's database.

2. The <user name> is entered incorrectly in the remote Authentication server's database.

[AUTH] ACE Node verification received; Client initialized.
The CyberSWITCH ACE client was in an initialized state. Node verification was received from the server and the initialization cycle is complete.

[AUTH] ACE No server configured for designated database location.
ACE is configured as a database location for security authentication. Either no ACE server has been configured or an error occurred when parsing the ACE server configuration.

[AUTH] RADIUS CHAP rejected for device: <device name>
The remote Authentication server rejected the CHAP mode authentication request for the indicated device. This usually indicates that one of the following has occurred:

1. The <device name> is not in the remote Authentication server's database.

2. The device's CHAP response was not calculated properly.

3. The device's SECRET does not match the secret in the RADIUS server's database.

4. The RADIUS server's database entry for this device contains errors.

[AUTH] RADIUS HDLC BRIDGE rejected bridge address: <mac address>
The remote Authentication server rejected the bridge address. This indicates that one of the following has occurred:

1. The <mac address> is not in the remote Authentication server's database.

2. The <mac address> is entered incorrectly in the remote Authentication server's database.

[AUTH] RADIUS INTERFACE LOOKUP rejected name <interface name>
The remote Authentication server route lookup feature rejected the interface name. This indicates that one of the following has occurred:

1. The < interface name> is not in the remote Authentication server's database.

2. The < interface name > is entered incorrectly in the remote Authentication server's database.

[AUTH] RADIUS IP HOST rejected IP Host id: <IP host Id>
The remote Authentication server rejected the IP Host id. This indicates that one of the following has occurred:

1. The <IP Host Id> is not in the remote Authentication server's database.

2. The <IP Host Id> is entered incorrectly in the remote Authentication server's database.

[AUTH] RADIUS IP RESOLVE rejected IP Address: <IP address>
The remote Authentication Server rejected the IP Address Resolution authentication request for the indicated IP Address. This usually indicates that one of the following has occurred:

1. The <IP Address> is not in the remote Authentication server's database.

2. The Authentication server's database entry for this IP Address contains errors.

[AUTH] RADIUS LOGIN rejected device: <device name>
The remote Authentication server rejected the named device. This indicates that one of the following has occurred:

1. The <device name> is not in the remote Authentication server's database.

2. The <device name> is entered incorrectly in the remote Authentication server's database.

[AUTH] RADIUS PAP rejected device: <device name>
The remote Authentication server rejected the PAP mode authentication request for the indicated device. This usually indicates that one of the following has occurred.

1. The <device name> is not in the remote Authentication server's database.

2. The device's PASSWORD did not match the password in the RADIUS server's database.

3. The RADIUS server's database entry for this device contains errors.

[AUTH] RADIUS ROUTE LOOKUP rejected IP address: <IP address>
The remote Authentication server route lookup feature rejected the IP address. This indicates that one of the following has occurred:

1. The <IP address> is not in the remote Authentication server's database.

2. The <IP address> is entered incorrectly in the remote Authentication server's database.

[AUTH] Security data buffer allocated successfully
The Authentication agent was able to allocate and initialize all memory required to perform authentication requests.

[AUTH] Security data buffer allocation failed
The Authentication agent was not able to allocate and initialize all memory required to perform authentication requests. No authentication request will be attempted. Contact your Distributor or Customer Support.

[AUTH] TACACS LOGIN rejected user: <user name>
The remote Authentication server rejected the named user. This indicates that one of the following has occurred:

1. The <user name> is not in the remote Authentication server's database.

2. The <user name> is entered incorrectly in the remote Authentication server's database.

[AUTH] TACACS No server configured for designated database location.
TACACS is configured as a database location for security authentication. Either no TACACS server has been configured or an error occurred when parsing the TACACS server configuration.

[AUTH] Warning code: 0001 Timeout
The configured authentication server(s) did not respond to requests for user authentication. Either the authentication server is not up and running, or it cannot access the IP address.

[AUTH] Warning code: 0002 Missing required attribute from server
The response message from the authentication server did not provide all required attributes for user authentication. The attributes required vary, depending on type of service, and type of security. Refer to the RADIUS Authentication Server User's Guide for details. Then check user entry for all required attributes.

[AUTH] Warning code: 0003 No UDP buffer available
Internal resources were not available to send / receive an authentication message. Contact your Distributor or Customer Support.

[AUTH] Warning code: 0004 No authentication node available
Internal resources were not available to initiate an authentication session. Contact your Distributor or Customer Support.

[AUTH] Warning code: 0005 No host configured for server IP address
The System does not have a network route to the configured authentication server(s). Verify that a static route has been set up. Then, check your configuration for the correct addresses on interfaces and authentication server.

[AUTH] Warning code: 0006 UDP system failed
Internal resources were not available to initiate an authentication session. Contact your Distributor or Customer Support.

[AUTH] Warning code: 0007 Authentication mode mismatch
An internal request for authentication server access request occurred, but the System is configured in the on-node device table mode. Contact your Distributor or Customer Support.

[AUTH] Warning code: 0008 Authentication agent not initialized
The System could not obtain enough internal resources for the user authentication operation. Contact your Distributor or Customer Support.

[AUTH] Warning code: 0009 Server failed message digest test
A message received from the authentication server did not have the correct authenticator field value.

[AUTH] Warning code: 0010 Received unexpected authentication response code from server
A message was received from an authentication server that contained an invalid response message identifier.

[AUTH] Warning code: 0011 An unexpected server responded to the access request
An access response message was received from an authentication server that is not configured in the System.

[AUTH] Warning code: 0012 UDP call back processed with no data present
A message was received from an authentication server that contained zero data bytes.

Bad auth result in smgrauth_aa_notify for device <device name>
There was no device configured (on-node or in CSM) for the login id entered at the user-level security prompt in the terminal server interactive window. Check configuration.

Bad context on SccDatInd <context value>
Indicates a problem has occurred in forwarding frames from the hardware to the frame relay software. The intended context for this frame is specified by the indicated context value. Contact your Distributor or Customer Support.

Bad context on X25SccDatInd <context value>
A data packet has been received with an incorrect context. This indicates that the system allocation of SCC controllers is not in a consistent state. Restart the system.

Bad FR Frame Size = <frame size>
Indicates that a frame was received with an invalid length size. Contact your Distributor or Customer Support.

Baud Rate is <value> bps
The Autobaud procedure has terminated and the RS232 port has been set to the specified baud rate.

[BIF] Could not allocate memory for buffer queue
[BIF] Initialization failed
These messages appear together in the report log. They indicate that an error occurred during initialization of the Bridge Local Interface (which is required for IP Host mode). If these messages are present in the log, the system will not operate correctly. Please contact your Distributor or Customer Support.

Booting System Software
The Second Stage Boot is attempting to load and execute the System software.

Bootstrap came alive on DM card in slot <slot #>
Informational message stating that the initialization of the Digital Modem card was successful.

Bootstrap came alive on WAN card in slot <slot #>
Informational message during a successful system initialization. Download process update for WAN card in slot <slot #>. This should be reported after the "Bootstrap loaded...waiting for response" message for a given adapter.

Bootstrap loaded on WAN card in slot <slot #>, waiting for response...
Informational message during a successful system initialization. The first of three messages providing the download process status for WAN card in slot <slot #>.

Bridge is operating in RESTRICTED mode
Bridge is operating in UNRESTRICTED mode
One of the above messages will be displayed to indicate the configured Bridge mode of operation.

Calculating CRC's.....
An X-Modem transfer has been completed and the received data is being checked for integrity.

Callback type <call back type ID> is not currently supported.
During callback negotiation between the CyberSWITCH and the remote device, an unsupported type of callback was received.

Call control detected near end problem - Slot=<slot #> Port=<port #>
The system detected a problem when initiating a call over the indicated line. The call will be retried over a different line if possible.

Call_ID in use in HOST_CALL_REQUEST
An error has been detected in the R2 or RBS signaling procedure, which typically results in a failed call. Contact your Distributor or Customer Support.

Calling Line ID Failure, Duplicate ID - <calling line Id>
A call has come in for a device that is using Calling Line Id (CLID) as the only authentication method, and the given CLID is not unique across all devices.

Calling Line ID Security Failure <calling line Id>
The system has rejected a device due to a mismatch between the Calling Line Id presented by the caller and the Calling Line Id in the on-node device database or obtained via an off-node authentication server such as RADIUS.

Calling Line ID Security Failure <calling line Id>, Device: <device name>
The system has rejected a device due to a mismatch between the Calling Line Id presented by the caller and the Calling Line Id in the on-node device database or obtained via an off-node authentication server such as RADIUS. The device's name is also contained within the database.

Calling Line ID Security Failure - off-node authentication server not supported
The system authentication type is configured to obtain device information off-node, for example from a RADIUS server; however, such transactions are not yet supported when Calling Line Id Security is enabled.

Call Rejected, Maximum Bandwidth already in place to Device Id <device Id>
An incoming call was rejected because the Maximum Data Rate parameter was exceeded for the indicated device. The Maximum Data Rate parameter can be configured for PPP devices under the configuration utility CFGEDIT or through the Manage Mode.

Call Rejected, No Called TN IE
The switch did not deliver an Information Element for the call. This problem normally occurs if you are connected to a point-to-point line and have the System configured for a multipoint line. If you are connected to a multipoint line and get this message, call your phone company and report the problem.

Call Restrictions have been disabled by user command
The user has disabled Call Restrictions via the `callrest off` Dynamic Management command.

Call Restrictions have been enabled by user command
The user has enabled Call Restrictions via the `callrest on` Dynamic Management command.

Call Restriction statistics reset for new day
Call Restriction device information.

Call Restriction statistics reset for new month
Call Restriction device information.

Call Restrictions will allow calls to be made this hour
Call Restriction device information.

Call Restrictions will allow calls, but this hour is restricted
Calls are restricted during this hour but the action configured is to "Warn". Calls are still being allowed.

Call Restrictions will allow calls to be made
A Call Restriction limit has been exceeded but calls will still be allowed.

Call Restrictions will no longer allow calls to be made
A Call Restriction limit has been exceeded and calls will no longer be allowed. Existing calls will NOT be forced down.

Call Restrictions will not allow calls to be made this hour
Call Restriction device information.

Call Summary for <day/month/year> - Calls/Day=x Calls/Mth=x Mins/Day=x Mins/Mth=x
Call Restriction device information. Displays daily / monthly call totals at the end of a day or a month.

Cannot make Bridge Dial Out call. No device found.
Check configuration to insure that device is properly configured.

Can only do SPEECH and 3.1K AUDIO calls in HOST_CALL_REQUEST
An improper outgoing call was attempted on an RBS line. Ensure that the device that is being called is a digital modem device and ensure that the "dm" flag has been added to peer calls.

Can't call Dial Out User. Security is not Device Level.
Check configuration. Bridge Dial Out requires device-level security and a properly configured Device List.

Can't start offnode server lookup of Dial Out User.
CyberSWITCH unable to send out a request to the off-node server. One of two possibilities: there may be problems communication on the LAN, or the server may not be configured properly. Verify LAN connectivity with server, and then check to see if server configured properly.

Calls Active
xx Active Sites
Current number of sites connected.

Calls Active
xxx to <sitename>
Bandwidth to each site.

Capability description processing error - <caperror>.
System is in minimal configuration mode.
A problem has occurred during system installation. The <caperror> will further identify the problem:

- *File not found*
- *Could not open file*
- *File already exists*
- *Header corruption*
- *File write problem*
- *Hash key mismatch*
- *Invalid serial number*
- *Invalid capability type*
- *Invalid capability format*
- *Invalid capability value*

The system will come up in a minimal capability mode, allowing only one physical connection, one X.25 virtual connection, and one Frame Relay virtual connection. Contact your Distributor or Customer Support.

Note: Duplicating serial numbers on all systems is a license violation.

Capability upgrade processing error - <caperror>.
Upgrade file was ignored.
A problem has occurred during system upgrade. The <caperror> will further identify the problem:

- *File not found*
- *Could not open file*
- *File already exists*
- *Header corruption*
- *File write problem*
- *Hash key mismatch*
- *Invalid serial number*
- *Invalid capability type*
- *Invalid capability format*
- *Invalid capability value*

The system will revert to its original level and the upgrade process will not be allowed. Contact your Distributor or Customer Support.

Note: Duplicating serial numbers on all systems is a license violation.

Cause <cause code> received for DLCI <dlci index>
A CLLM message was received indicating that the PVC associated with the indicated DLCI is subject to the event denoted by the indicated cause code. These events are listed below with their corresponding cause code:

Cause Code	*Event*
2	Mild congestion
3	Severe congestion
7	Fixed fault notification: facility / equipment failure
10	Discard all frames: maintenance action in progress

CB disconnect:(1) Password Incorrect
CB disconnect:(2) Call-back number not found
CB disconnect:(3) Ethernet address inconsistent
CB disconnect:(4) Disconnecting for Call-back
CB disconnect:(5) Invalid Packet Received
CB disconnect:(6) Unable to resolve protocols
CB disconnect:(7) Inband Timeout
CB disconnect:(8) Line Integrity Violation
CB disconnect:(?) Unspecified
For all of the above Combinet generated messages, the Combinet has disconnected for the indicated reason. Check your Combinet configuration, and adjust if necessary. If problem persists, contact your Combinet distributor.

[CCP] Internal Decompression Failure
The system was unable to decompress a packet though the frame was delivered properly from a protocol perspective. This is an unexpected condition with a properly functioning device implementation and is thus considered a unrecoverable error. The system will close the CCP protocol, meaning that the connection continues to operate, but in an uncompressed mode.

[CCP] Option Negotiation Failure, Non-Convergence detected
During PPP negotiation, the system attempted to negotiate CCP, but it was not possible to arrive at a mutually acceptable set of protocol parameters with the connected device. The connection continues to operate, but without compression.

The cause of this problem may result from:
- the system has too little memory to support compression, or
- the two devices involved don't agree on which bridging / routing protocol to use (due to a mis-configuration)

Check configuration for correct protocol. If this is not the problem, check memory availability.

CDR was unable to obtain a buffer to report a CDR event
A buffer was unavailable to send a call detail recording event log message, and the message was discarded. This message is logged once when the condition first occurs. It will not be logged again until the condition has been cleared and CDR has successfully obtained a buffer. If the condition occurs again later, another message will be logged.

CHANNEL in use in HOST_CALL_REQUEST
An error has been detected in the R2 or RBS signaling procedure, and will typically result in a failed call. If problem persists, contact your Distributor or Customer Support.

[CHAP] Authentication Failure of remote device <device name> - <error message>
On-node or off-node (for example, through the RADIUS Server) CHAP authentication has failed. The <*device name*> will contain the device name configured in the Device Table. The <error message> will contain information that should aid in trouble shooting.

If the authentication failure is an on-node failure, the <error message> will contain one of the following strings:

Challenge Response failed hash calculation
No Secret configured in Device Table
Name not configured in Device Table
Invalid information in authentication attempt

If the authentication failure is an on-node failure, the <error message> will contain one of the following strings:

Challenge Response failed in hash calculation
No Secret configured in Device Table
Name not configured in Device Table

If the authentication failure is an off-node failure, the remote Authentication Agent will generate the error message.

[CHAP] Authentication Failure - remote device not responding
The System has not received a challenge response from the peer. The cycle is attempted the configured number of times, after which a failure is declared. Check your remote device.

[CHAP] Authentication Failure - unable to initiate server transaction <return code>
The System authentication type is configured to obtain device information off-node, for example from a RADIUS server, but an internal error has prevented the transaction from occurring. Check the Radius Server report log for more information. If unsuccessful, contact your Distributor or Customer Support.

[CHAP] Remote device indicates Authentication Failure of system <data>
The System received a fail reply in remote CHAP mode. This means that the System has not been authenticated by the peer, and most likely the link will be released. <data> contains a portion of the received frame, which should aid in trouble shooting the situation.

Circuit-mode/Packet-mode aggregation will not be allowed,
dropping oldest connection to site <site name>
This message may appear if switched calls are used to back up Frame Relay. If this message is seen infrequently, it merely indicates the changeover from Frame Relay to switched calls and back again. If this message is seen frequently, contact your Distributor. At the same time that these messages are displayed in the log, an open Monitor Connection window may show brief periods (<1 second) where the indicated Bandwidth suddenly increases and then decreases. This is due to the changeover between Frame Relay and switched calls and is not a problem.

CNTR-TMR:Timed out waiting for TMR <number> interrupt!
The i386s specified timer did not respond during a POST testing its interrupt capabilities. The boot process should continue; however, make note of the error message in the event of a future problem.

Configured adapter #'x' type does not exist
The interface adapter indicated does not match the resource configuration in the system. Correct the configuration on the system.

Connection disconnected for license violation
A connection was disconnected because there were more connections in place than allowed with your version of the system software. A larger software version should be ordered.

Could not find peer in ip_wan_device_connected
IP reported a new IP stream to RADIUS Accounting, and RADIUS Accounting does not have any record of this peer. Contact your distributor or Customer Support.

Could not find peer in Stop_accounting_Session
This condition occurs if RADIUS Accounting is enabled while a call is up, and then the call disconnects. This situation is normal. However, if this occurs at any other time, a problem may exist. Contact your distributor or Customer Support.

Could not find port for static route with next hop address <AppleTalk Address>
Contact your distributor or Customer Support.

Could not get Call Restriction information
Contact your Distributor or Customer Support.

Could not get current monthly charges information
Could not get the current monthly call charge information on the system. The call charge feature will be disabled and the problem should be reported. Contact your Distributor or Customer Support.

Could not obtain fcr packet buffer
AppleTalk related. Contact your distributor or Customer Support.

Couldn't find speech service - <slot #, port #>
An incoming call was received which specified Speech Bearer Service capability. Speech service is not currently supported with the System. Most likely, the incoming call was a wrong number. The system will attempt to treat the call as 56 Kbps data.

CSM at <IP address> is now being used as PRIMARY.
The device at the indicated IP addressed is now acting as a primary CSM service. The primary service is selected through the CSM GUI. When configuring services, you first add an entry for each service, then optionally configure managing information to designate primary and secondary services for the network's Access Servers.

Current monthly charges reset for new month
Reported on the first day of the month to indicate that the current monthly call charges value is being reset to zero.

Data link down: Slot=<slot #> Port=<port #> Ces<communication endpoint suffix>
The data link on the specified line is down. If all the data links for a line are down, the line is disabled for switched connection use.

Data link test successful: DSL <port #>, CES 1
This message applies for 1TR6 BRI only. If Layer 1 is established, a test will be done to determine if the data link can be established. This message indicates successful test results.

Data link up: Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix>
The data link on the specified line is active and can be used for establishing switched connections.

DCE Data Rate is invalid on FrStartPVC
The user has configured a data rate which is inconsistent with the application. This can only happen with serial lines such as V.35 where the data rate must be specified in bits-per-second and the configured rate is not valid.

Dedicated connection down: <slot #, port #>
The dedicated connection is down. Switched backup connections will be used, if available. This message will occur if the other system is down, or if the network interface line is not connected, or if the authentication of the remote device failed.

Dedicated connection to device <device name> up: <slot #>,<port #>
The indicated dedicated connection is operational.

[DHCP-P] Failed to close UDP port after terminating last DHCP client
An internal error occurred in the DHCP Proxy Client. When all DHCP client invocations are terminated, the UDP ports used by the DHCP Proxy Client should be closed. Contact your Distributor or Customer Support.

[DHCP-P] Failed to close UDP port (x), erc = <y>
This message appears when the DHCP Proxy Client is being disabled from Manage Mode and it encounters an error while trying to close one or both of the UDP ports that it has open. Contact your Distributor or Customer Support.

[DHCP-P] Failed to de-register with the IP Address Pool Manager, erc = <x>
This message indicates that a failure was encountered by the DHCP Proxy Client while it was being disabled. It was unsuccessful in its attempt to de-register as a provider of “DHCP” addresses for the IP Address Pool. Contact your Distributor or Customer Support.

[DHCP-P] Failed to open UDP port for first DHCP client
An internal error occurred in the DHCP Proxy Client. When the first DHCP client invocation starts, the UDP ports used by the DHCP Proxy Client should open. Contact your Distributor or Customer Support.

[DHCP-P] Failed to open UDP port (x), erc = <y>
This message appears when the DHCP Proxy Client is being enabled and it encounters an error while trying to open one or both of the UDP ports that it requires for operation. Contact your Distributor or Customer Support.

[DHCP-P] Failed to register with the IP Address Pool Manager, erc = <x>
This message indicates that a failure was encountered by the DHCP Proxy Client while it was being enabled. It was unsuccessful in its attempt to register as a provider of “DHCP” addresses for the IP Address Pool. Contact your Distributor or Customer Support.

[DHCP-P] Ignoring offers from DHCP server x.x.x.x; the server MUST be on a primary LAN interface, or IP addresses will not be obtained
In order for the DHCP proxy client to successfully obtain IP addresses for multiple interfaces, the DHCP server must reside on a primary LAN interface. If it does not, this message is written to the Report Log, and no IP addresses will be obtained from the server and placed into the IP Address Pool. To correct, use CFGEDIT to change the DHCP server's interface from a secondary interface into a primary interface for that LAN port.

[DHCP-P] Invalid DHCP Server LAN port encountered in configuration; NIF entry not activated
This message appears when the DHCP Proxy Client encounters an invalid configuration setting for an IP network interface's LAN port on which the DHCP server is to be reached. This will result in no IP addresses being obtained for the network interface in question. Contact your Distributor or Customer Support.

[DHCP-P] Proxy Client disabled
This message indicates that the DHCP Proxy Client has been successfully disabled. This message will appear after the DHCP Proxy Client has been disabled from Manage Mode.

[DHCP-P] Proxy Client enabled
This message will appear whenever the DHCP Proxy Client has been successfully enabled. This could be during system initialization (if configuration values have enabled it), or after the DHCP Proxy Client has been enabled from Manage Mode.

[DHCP-P] Proxy Client initialization failed
This message indicates that the DHCP Proxy Client did not initialize successfully. The DHCP Proxy Client will not be operational. Contact your Distributor or Customer Support.

[DHCP-P] UDP port (67) closed
The DHCP Proxy Client is being disabled from Manage Mode and it must close the BOOTPS UDP port (port 67). If the DHCP Relay Agent is enabled, the BOOTPS port must remain open. If this is the case, the DHCP Proxy Client will not close the UDP port.

[DHCP-P] UDP port (67) opened
The DHCP Proxy Client is being enabled and it must open the BOOTPS UDP port (port 67). This may occur during system initialization, or after the DHCP Proxy Client has been enabled from Manage Mode. If the DHCP Relay Agent is also enabled, it may not be necessary for the Proxy Client to open this UDP port.

[DHCP-P] UDP port (68) closed
The DHCP Proxy Client is being disabled from Manage Mode and it must close the BOOTPC UDP port (port 68).

[DHCP-P] UDP port (68) opened
The DHCP Proxy Client is being enabled and it must open the BOOTPC UDP port (port 68). This may occur during system initialization, or after the DHCP Proxy Client has been enabled from Manage Mode.

[DHCP-R] Failed to allocate memory for transmit buffer pool
The system was unable to allocate memory for the DHCP Relay Agent's transmit buffer pool during initialization. The Relay Agent will not become operational. Contact your Distributor or Customer Support.

[DHCP-R] Failed to close UDP port (67), erc = <x>
An error occurred while the device was trying to disable the DHCP Relay Agent from Manage Mode. Contact your Distributor or Customer Support.

[DHCP-R] Failed to open UDP port (67), erc = <x>
An error occurred while attempting to enable the DHCP Relay Agent. The Relay Agent must open the BOOTPS UDP port in order to operate successfully. If this port could not be opened, the Relay Agent will not be enabled. Contact your Distributor or Customer Support.

[DHCP-R] Relay Agent disabled
The DHCP Relay Agent has been successfully disabled. This message will appear if the user disabled the Relay Agent from Manage Mode.

[DHCP-R] Relay Agent enabled
The DHCP Relay Agent has been successfully enabled. This could be during system initialization (if configuration values have enabled it), or after the DHCP Relay Agent has been enabled from Manage Mode.

[DHCP-R] Relay Agent initialization failed
This message indicates that the DHCP Relay Agent did not initialize successfully. The Relay Agent will not be operational. Contact your Distributor or Customer Support.

[DHCP-R] UDP port (67) closed
The DHCP Relay Agent is being disabled from Manage Mode and it must close the BOOTPS UDP port (port 67). If the DHCP Proxy Client is also enabled, the BOOTPS port must remain open. In this case, the DHCP Relay Agent will not close the UDP port.

[DHCP-R] UDP port (67) opened
The DHCP Relay Agent is being enabled and it must open the BOOTPS UDP port (port 67). This may occur during system initialization, or after the DHCP Relay Agent has been enabled from Manage Mode. If the DHCP Proxy Client is also enabled, it may not be necessary for the Relay Agent to open this UDP port.

Dial Out Device does not have Bridge Callable Enabled
Check configuration. Enable the *Make Calls for Bridge Data* field under *Device Table Menu, Bridging*.

Discrepancy in dynamically-obtained device data
The System authentication type is configured to obtain device information off-node. In an outbound call scenario with security enabled, two transactions may occur for the same device. If these do not yield the same information, the call is dropped. Contact your Distributor or Customer Support.

DL <slot #, port #, ces> Down
The specified data link for a line is down and considered unusable. Refer to the log error messages for further information (`dr` command).

DM card in slot <slot #> has no firmware
While attempting to initialize the Digital Modem card, the system registered an invalid firmware state. Contact your distributor or Customer Support. You most likely need to replace or upgrade the firmware on the Digital Modem.

DM card failed FLASH download bad xx SREC
The Digital Modem card has failed the firmware update due to a corrupt file. Contact your Distributor or Customer Support.

DM card in slot <slot #> has bad FLASH
The FLASH memory on the Digital Modem card has been identified as bad during an attempt to update or access it. Contact your Distributor or Customer Support.

DM card in slot <slot #> in unknown state
The Digital Modem card is in an unrecognizable state. Reseat the card in its ISA slot, and / or check the MVIP cabling. If the problem persists, contact your Distributor or Customer Support.

DM card in slot <slot #> is not functional
The system was unable to initialize the Digital Modem in the specified slot correctly. Check all switch and / or jumper settings on the board to ensure they match the values in CFGEDIT. If the board is configured properly, and this message still appears, contact your Distributor or Customer Support.

DM card in slot <slot #> will receive new firmware
Informational message stating that the system has detected that the current firmware of the specified modem is a lower revision level than what is supported in the currently installed software. For 56K modem technology, the system will attempt to update the card. For modem technology other than 56K, the upgrade command must be used to upgrade the firmware revision. Watch for subsequent log messages to ensure the update is successful.

DM card in slot <slot #> failed FLASH download
The system has failed to successfully update the firmware revision of the Digital Modem card. Contact your Distributor or Customer Support.

DM card in slot <slot #> FLASH download complete
Informational message stating that the system has successfully updated the firmware present on the Digital Modem card.

DM card in slot <slot #> is initializing
Informational message when digital modem card first powers up; card in process of initializing.

DM card in slot <slot #> is not usable, could not upgrade
The modem firmware upgrade process failed for this card. Call your Distributor or Customer Support.

DM card in slot <slot #> is reinitializing
This message may display after the system attempts a Digital Modem initialization on power up. If the system determines the Digital Modem card needs new firmware, or if the Digital Modem did not initialize correctly, it will try again. Watch for subsequent log messages to determine if a course of action is necessary.

DM card in slot <slot #> signals it is operational
Informational message stating that the Digital Modem is now ready for use.

DM card type configured in slot <slot #> does not exist
Using the resource database, the system has tried to initialize a Digital Modem card that doesn't exist. Check all switch and / or jumper settings on the board to ensure they match the values in

CFGEDIT. If the board is configured properly, and the message still appears, contact your Distributor or Customer Support.

DM card in slot <slot #> will not come out of reset
There are problems initializing the board. Contact your Distributor or Customer Support.

DM upgrade timeout. Board=<board #>, Modem=<modem #>
DM upgrade error during download. Modem says = xxx
DM upgrade no response at start. Board=<board #>, Modem=<modem #>
DM upgrade flash erase failed. Board=<board #>, Modem=<modem #>
DM upgrade no response at end. Board=<board #>, Modem=<modem #>
There were problems while attempting to update the firmware of the specified modem due to either a corrupt firmware file or hardware problems. Reseat the card in its ISA slot, and/or check the MVIP cabling. If problems persist, contact your Distributor or Customer Support.

DM upgrade started. Board=<board #>, Modem=<modem #>
The system has begun to update the firmware of the specified modem on the Digital Modem card. Watch for subsequent log messages to ensure the update is successful.

DM session in unknown upgrade state. Board=<board #>, Modem=<modem #>
There were problems while attempting to update the firmware of the specified modem due to either a corrupt firmware file or hardware problems. Contact your Distributor or Customer Support.

DM upgrade success. Board=<board #>, Modem=<modem #>
The system has successfully updated the firmware of the specified modem on the Digital Modem card.

DM: TimeSlot driver circuit id already in use on CREATE
DM: No TimeSlot driver circuits available for CREATE
DM: TimeSlot driver circuit id not in use on REMOVE
DM: TimeSlot driver circuit id not found on REMOVE
There were problems related to the Digital Modem's use of the TDM bus. Contact your Distributor or Customer Support.

Downloading Bootstrap to DM card in slot <slot #>
Informational message stating that the system is attempting to initialize a Digital Modem card. Watch for subsequent log messages to ensure the initialization is successful.

Downloading DM card in slot <slot #> with operational software
Informational message displayed during a successful initialization. Watch for subsequent log messages to ensure the initialization is successful.

Downloading WAN card in slot <slot #> with operational software
Informational message during a successful system initialization. The status of the download process for WAN card in slot <slot #> is identified. This should be reported after the "Bootstrap came alive..." message for a given adapter.

DSL test failed to establish Layer 1, port=<port #>
During power up, all WAN lines undergo a test to see if Layer 1 can be established. This message indicates a test failure. Check the wiring. If correct, contact your phone company.

Duplicate Calling Line ID <Calling line Id> detected for devices <device name> and <device name>
This message is logged at system initialization if any devices are found to share duplicate Calling line Ids, and have no other authentication method. This problem should be corrected by adding additional authentication method(s) to the necessary device(s).

Each mandatory connection uses xx bytes
There is not enough memory available to accommodate the system's total capacity load. This informational message identifies how much memory is needed to add an additional mandatory connection.

Each optional connection uses xx bytes
There is not enough memory available to accommodate the system's total capacity load. This informational message identifies how much memory is needed to add an additional optional connection.

ECP negotiation failed to converge
Verify compatible encryption parameters on each side of the link.

EDRV transmit error <error code>
An error was returned upon the software's request to transmit a data frame. Contact your Distributor or Customer Support.

EDS-DES Board Absent
EDS-FEAL Board Absent
The encryption board is either physically not in the backplane, or the dip switches on the board are set incorrectly. Check for the board; verify the *switch settings*.

Error closing file 's'
The WAN card initialization subsystem encountered an error while downloading a WAN card. The system could not close the download disk file indicated. Restart the system. If the error continues, Contact your Distributor or Customer Support.

Error closing file <file name>, slot <slot #>
Error closing password data file
If seen repeatedly, the above messages indicate a problem with your hard drive. Please contact your Distributor or Customer Support.

Error downloading bootstrap program to adapter #'x'
The WAN card initialization subsystem encountered an error on the indicated adapter while downloading the bootstrap program. Restart the system and review the configuration for the adapter. If the problem persists, the indicated adapter card may be faulty; contact your Distributor or Customer Support.

Error downloading operational software to adapter 'x'
The WAN card initialization subsystem encountered an error on the indicated adapter while downloading operational software. Restart the system and review the configuration for the adapter. If the problem persists, the indicated adapter card may be faulty and you should contact your Distributor or Customer Support.

Error during channel initialization Access <access index>
An error has occurred during the initialization of the indicated Frame Relay Access, or port. Likely cause of this entry is that the system has run out of memory. Contact your Distributor or Customer Support.

Error during port initialization Access <access index>
An error has occurred during the initialization of the indicated Frame Relay Access, or port. Likely cause of this entry is that the system has run out of memory. Contact your Distributor or Customer Support.

Error during PVC initialization Access <access index>
An error has occurred during the initialization of the indicated. Likely cause of this entry is that the system has run out of memory. Contact your Distributor or Customer Support.

Error initializing WAN card: <WAN card Id>
The system could not initialize the specified WAN card during system initialization. Check the WAN card installation and configuration. If the error continues, report the problem.

Error in last LMI message detected Error <error code>
An error was detected in the last LMI message forwarded by the network. The error is identified by the indicated error code.

Error loading WAN board, data verify error: adapter 'x'
The WAN card initialization subsystem encountered an error during download verification. The specified adapter card may be faulty. Contact your Distributor or Customer Support.

Error mapping WAN adapter #'x' into Host memory map
The configured memory location of the indicated WAN card conflicts with another WAN card or device. Review the configuration for the indicated adapter.

Error opening file <file name>
Error opening file <file name>, section = <section name>
Error opening file <file name>, slot <slot #>
If seen repeatedly, contact your Distributor or Customer Support.

Error parsing old WAN (Direct Host) interface: bad format
The information contained in the WAN (Direct Host) interface is invalid. To correct, use CFGEDIT to reconfigure the interface.

Error initializing WAN card: <WAN card Id>
The system could not initialize the specified WAN card during system initialization. Check the WAN card installation and configuration. If the error continues, report the problem.

Error parsing old WAN (Direct Host) interface: LAN interface <LAN netif name> for specified port <port#> already in use
This error may display after upgrading software which contains secondary IP addressing and an "old" style WAN (Direct Host) interface. To correct, use CFGEDIT to delete any WAN (Direct Host) interfaces on the problematic LAN port, and reconfigure them.

Error parsing old WAN (Direct Host) interface: no LAN interface for specified port <port#>
This error may display after upgrading software which contains secondary IP addressing and an "old" style WAN (Direct Host) interface. To correct, use CFGEDIT to delete the problematic WAN

(Direct Host) interface. Afterwards, configure a LAN interface and then read the WAN (Direct Host) interface.

Error parsing WAN (Direct Host) interface: no LAN interface for specified name <name>
The LAN network interface associated with this WAN (Direct Host) interface is not present. Use CFGEDIT to delete the problematic WAN (Direct Host). Check configuration for the suspect LAN interface; it most likely will not be there. Add LAN interface, then reconfigure the WAN (Direct Host) interface.

Error opening file \system\ethernt2.bin
The LAN adapter executable file could not be opened. Check for proper software installation.

Error programming adapter #'x' hardware
The WAN card initialization subsystem encountered an error while attempting to program the hardware on the indicated adapter. Restart the system and review the configuration for the adapter. If the problem persists, the indicated adapter card may be faulty; contact your Distributor or Customer Support.

Error reading file <file name>, section = <section name>
If seen repeatedly, the above message indicates a problem with your file system. Contact your Distributor or Customer Support.

Error reading file \system\ethernet2.bin,section = <file type>
The specified section of the LAN adapter executable file could not be read. Check for proper software installation.

Error reading platform type: couldn't open file C:\SYSTEM\PLATFORM.NEI
Error reading platform type: error reading C:\SYSTEM\PLATFORM.NEI
Error reading platform type: there is no "plat name" field
Error reading platform type: there was no "=" in the string
Error reading platform type: type value is too large
Error reading platform type: type was not converted to an int
There is a problem with the platform.nei file. Reinstall the system Installation/Upgrade diskettes or CD-ROM.

Error reading sdconf.rec file
An error occurred during parsing of the ACE configuration file. The file was found, but did not have the expected format. Either repeat the download of the file from the ACE server, or reenter the ACE database location configuration and save changes using CFGEDIT.

Error requesting slot activation
Contact your Distributor or Customer Support.

Error sending message to Call Control
The system detected a failure while sending a message to the WAN adapter. Restart the system and review the resource configuration. If the error persists, contact your Distributor or Customer Support.

Event <event code> occurred on FR Access <access index>, DLCI <dlci index>
A debug message logged to indicate Frame Relay events occurring for the indicated DLCI on the indicated Access. The event is given in both textual, event, and numeric, code, forms.

Facility not subscribed - Slot=<slot #> Port=<port #>
This probably indicates a SPID configuration error on the indicated line. The configuration should be corrected on the system or the switch.

Failed to allocate enough memory for XILINX load file
The WAN card initialization subsystem failed to allocate a buffer for use in downloading files. Restart the system. If the problem continues, contact your Distributor or Customer Support.

FAILED TO BOOT SYSTEM SOFTWARE
While attempting to load the System software, an error was detected. The system will automatically reset and attempt a reboot in an effort to correct the problem. If the system continues to fail, make note of the displayed messages, and contact your Distributor or Customer Support. A software update is likely needed.

FAILED TO FORMAT RFA
The Flash File System could not be formatted. The system will automatically reset and attempt a reboot in an effort to correct the problem. If the system continues to fail, make note of the displayed messages, and contact your Distributor or Customer Support. A software update is likely needed.

Failed to get a tone signaling session
An error has been detected in the R2 signaling procedure, and will typically result in a failed call. The error was due to unrecognizable or incorrect information. If problem persists, contact your Distributor or Customer Support.

FAILED TO INSTALL XMODEM FILESET INTO FLASH MEMORY
While writing a file into the Flash File System, an error was detected. The system will automatically reset and attempt a reboot in an effort to correct the problem. If the system continues to fail, make note of the displayed messages, and contact your Distributor or Customer Support. A software update is likely needed.

Failed to obtain Terminal info in smgr_proc_terminal_auth_sess 0
A session control block was not found for this authentication session. Contact your Distributor or Customer Support.

Failed to start a Terminal Auth session. Device + User level Security not enabled
A terminal mode connection was received and Device + User level security was not enabled. Verify correct security settings and default async protocol settings.

FAILED XMODEM INITIALIZATION
The UART controlling the Console Information Port (CIP) could not be initialized. The system will automatically reset and attempt a reboot in an effort to correct the problem. If the system continues to fail, make note of the displayed messages, and contact your Distributor or Customer Support. A software update is likely needed.

FAILED XMODEM SESSION
The X-Modem session did not successfully terminate. Likely causes include exhausting timeout limits and noisy lines. The system will automatically reset and attempt a reboot in an effort to correct the problem. If the system continues to fail, make note of the displayed messages, and contact your Distributor or Customer Support. A software update is likely needed.

Failure during read of file <file name> for WAN card in slot <slot #>
If seen repeatedly, the above message indicates a problem with your hard drive. Contact your Distributor or Customer Support.

Failure during read of file 's'
The WAN card initialization subsystem encountered an error reading the file indicated. Check for proper software installation.

Failure during Static RAM test on adapter #'x'
The WAN card bootstrap program encountered an error during the Static RAM test. This indicates that the adapter card may be faulty. Contact your Distributor or Customer Support.

Failure on closure of file <file name>
Failure on file closure <file name>
Failure on write of file <file name>
Failure opening file <file name>
If seen repeatedly, the above messages indicate a problem with your hard drive. Contact your Distributor or Customer Support.

Failure to allocate enough memory for XILINX load file
The WAN card initialization subsystem failed to allocate a buffer for use in downloading files. Restart the system. Report the problem if it continues.

File=l2, Fn=<func name>, err=Layer 2 Error<err msg>, port=<port#>, CES=<link Id>
A Layer 2 error was encountered on the indicated BRI link or port. Your ISDN line (data link) may be going down. If this error condition persists, contact your Distributor or Customer Support. Below are possible error messages and their corresponding definitions:

DISC rcvd
The Network has sent a Layer 2 DISC (Disconnect), terminating the data link. An attempt will be made to re-establish the data link after a switchtype-dependent delay.

DM rcvd
The Network will not allow establishment of the data link at this time. An attempt will be made to re-establish the data link after a switchtype dependent delay.

MDL_ERR_RESP rcvd
The Network has not responded to TEI requests - no data link was established. An attempt will be made to re-establish the data link after a switchtype dependent delay.

rcvd MDL_REM_REQ for TEI <TEI value>
The network has removed the specified TEI, terminating the data link. An attempt will be made to re-establish the data link after a switchtype dependent delay.

File=ME, Fn=_mdl_err, err=Layer 2 Error<err code>rcvd, port=<port#>, CES<link Id>
A Layer 2 error was encountered on the indicated BRI link or port. Your ISDN line (data link) may be going down. If this error condition persists, then report the problem. Below are possible error codes and their corresponding definitions (based on Table 11-1 from CCITT Q.921 specification):

A
The Network sent a RNR (Receiver not Read) or REJ (Reject).

B, D
The Network sent a DM(F=1) or a UA and will not allow establishment of the data link at this time. An attempt will be made to re-establish the data link after a switchtype dependent delay.

C
The Network sent an unsolicited UA and will not allow establishment of the data link at this time. An attempt will be made to re-establish the data link after a switchtype dependent delay.

E
The Network sent a DM(F=0). The data link will be restarted immediately.

F
Network restarted data link.

H
Timeout on sending DISConnect to the Network. Unable to bring up data link. An attempt will be made to re-establish the data link after a switchtype dependent delay.

I
Timeout sending I(Info) frame to the Network. The data link will be restarted immediately.

J
The Network sent a Layer 2 frame with an incorrect receive sequence number (Nr).

K
The Network sent a FRMR (Frame Reject) response. The data link will be restarted immediately.

L
The Network sent a Layer 2 frame with a control field error. This is typically an unimplemented frame.

M
The Network sent a Layer 2 frame with an illegal Info field.

N
The Network sent a Layer 2 frame with an incorrect length.

O
The Network sent a Layer 2 frame that was too long.

U
The Network sent a Layer 2 frame with a control field error. Typically an unknown frame.

File Access Err
System unable to access file. Check for one of the following log error messages:

```
Error opening file <file name>
Error reading file <file name>, section = <section name>
Error opening file <file name>, slot <slot #>
Read 0 bytes from file <file name> for WAN card in slot <slot #>
Failure during read of file <file name> for WAN card in slot <slot #>
Error closing file <file name>, slot <slot #>
Error closing password data file
Error opening password data file
Failure on closure of file <file name>
Failure opening file <file name>
Failure on file closure <file name>
Failure on write of file <file name>
```

If you see any of these log messages repeatedly, there may be a problem with the file system. Contact your Distributor or Customer Support.

Formatting Flash Memory.....
The user has either requested the Flash to be formatted or a corrupted Flash File System was detected while attempting to save an upgrade/installation file set (transferred via X-Modem).

[FR_IETF] Authentication Failure of remote device NAME
[FR_IETF] Off-Node Authentication Failure of remote device NAME
The device database does not contain an entry for the device specified by NAME. Reconfigure either the PVC name or the device name so that they match.

[FR_IETF] detected PPP protocol from "NAME", shutting down PVC
FR_IETF has detected a configuration mismatch between the system and the remote device NAME. The administrator must change the PVC configuration on one of the devices.

Frame Relay event queue full
Indicates a lack of system resources to handle the level of traffic being experienced. Contact your Distributor or Customer Support.

Frame Relay PVC connection down: Slot=<slot number>, Port=<port number>
The Frame Relay PVC connection is down for the indicated slot and port number.

Frame Relay PVC connection up: Slot=<slot number>, Port=<port number>, DLCI=<DLCI index>
The Frame Relay PVC connection is up for the indicated slot, port, and DLCI index.

FrBufFree: error <error code> during free
The indicated error occurred during an attempt to free a buffer to its memory pool. Contact your Distributor or Customer Support.

FrUtl: No registered device for DLCI <dlci index>
A frame was received on the PVC associated with the indicated DLCI, and no Frame Relay Service Device had (as yet) registered to use this PVC.

IePvcStatus: Received Status Report for unknown PVC # <dlci index>
The indicated unknown DLCI was indicated in a STATUS message received from the network. This DLCI number is entered in the "unknown DLCI" list and can be displayed via the FR LMI system console command.

Incoming call from <Device Name>, Slot=<slot #>, Port=<port #>, Chan=<channel #> Rejected by BW Reservation
A bandwidth reservation message. Indicates that a call has come in from the indicated device, on a line that is not in this device's profile. The call will be disconnected. If you see this message often, check the remote device's configuration to prevent wasted calls.

Initial TDM Clock Master: <slot#, line#>
The external line indicated has been selected as the master clock source.

Initializing...
Displays the current state of the system (initialization).

Installing File Set into Flash Memory
The file set, received via X-Modem, has successfully passed its verification tests and is now being written into the Flash File System.

Insufficient space for buffer pool creation
There is not enough system memory to proceed with the creation of the requested size buffer pool. Contact your Distributor or Customer Support.

Interrupt fault on WAN Adapter in Slot <slot #>
The interrupt jumper for the WAN Adapter in the specified slot is missing or misplaced.

Invalid caller number: <caller's sites name> - <caller's number>
The incoming call security feature is enabled and a call was received from an unknown remote site, therefore the call was disconnected. If the call was from a valid remote site, the device list must be updated to include the remote site's phone number.

Invalid Call_ID in HOST_CALL_CONNECTED
Invalid Call_ID in HOST_CALL_DISCONNECT
An error has been detected in the R2 or RBS signaling procedure, which typically results in a failed call. The error was due to unrecognizable or incorrect information. If problem persists, contact your Distributor or Customer Support.

Invalid CLLM received on Access <access index>
An invalid CLLM message was received on the indicated Frame Relay Access. The message had either missing elements or invalid contents.

Invalid LAN Adapter identifier
The system has detected invalid LAN adapter hardware. Check for proper LAN adapter configuration and hardware installation.

Invalid Password <password> given
The remote Combinet sent a password that did not match any device table entries. This most likely is due to a configuration error. Check the configuration, and change the password.

Invalid return code from SIG_get_rsc_inbound
Invalid return code from SIG_get_rsc_outbound
An error has been detected in the R2 signaling procedure, and will typically result in a failed call. The error was due to unrecognizable or incorrect information. If problem persists, contact your Distributor or Customer Support.

Invalid SERIAL.001 file present, file is ignored.
Contact your Distributor or Customer Support.

Invalid SERIAL.BIN file present, system booting in minimal mode.
Contact your Distributor or Customer Support.

Invalid serial number in SERIAL.001, file is ignored.
Contact your Distributor or Customer Support.

Invalid serial number in SERIAL.BIN file, system booting in minimal mode.
Contact your Distributor or Customer Support.

IP Error from ESP datagram - discarded
An error occurred within the IP forwarding logic which make it impossible to send this datagram.
[IP] Invalid Device Info. Device is not IP callable <device name>
An IP packet could not be forwarded to a remote network because the next-hop device for that network is not configured as *IP Callable*. The CyberSWITCH returns a *network unreachable* message to the sender.

[IP] x.x.x.x not added to the pool: Invalid IP address
A failure was encountered by the IP subsystem during initialization processing. IP made an unsuccessful attempt to add a "static" address to the IP Address Pool. The IP address being added did not match any of the configured IP network interfaces.

[IP] x.x.x.x not added to the pool: Invalid Device Id
A failure was encountered by the IP subsystem during initialization processing. IP made an unsuccessful attempt to add a "static" address to the IP Address Pool. The ID supplied by the IP subsystem was invalid. Contact your Distributor or Customer Support.

[IP] x.x.x.x not added to the pool: IP Address Pool Full
A failure was encountered by the IP subsystem during initialization processing. IP made an unsuccessful attempt to add a "static" address to the IP Address Pool. The IP Address Pool was already full.

[IP] x.x.x.x not added to the pool: Unknown error (y)
A failure was encountered by the IP subsystem during initialization processing. IP made an unsuccessful attempt to add a "static" address to the IP Address Pool. An unknown error code was returned by the IP Address Pool Manager. Contact your Distributor or Customer Support.

[IPAP] ResMem returned invalid device maximum value (x)
A memory allocation failure was encountered by the IP Address Pool Manager during initialization processing. Contact your Distributor or Customer Support.

[IP] Cannot get system memory for xxxx
There is not enough system memory available for IP software to operate ("xxxx" is a variable name internally used). Contact your Distributor or Customer Support.

[IP] Cannot process incoming remote IP device <IP address>, no rsc avail
The IP software was unable to accept the incoming IP device to a WAN (Direct Host) interface because it could not obtain necessary resource. The WAN connection may remain for a while, but the remote IP device will not be able to communicate with any IP devices over WAN. Contact your Distributor or Customer Support.

[IP] Cannot start Proxy Arp for <IP address #>, no cmd buf avail
The IP software attempted to start the proxy arp for the IP device indicated by the <IP address #>, but was unsuccessful because it could not obtain necessary memory. Contact your Distributor or Customer Support.

[IP] Cannot stop Proxy Arp for <IP address #>, no cmd buf avail
The IP software attempted to stop the proxy arp for the IP device indicated by the <IP address #>, but was unsuccessful because it could not obtain necessary memory. Contact your Distributor or Customer Support.

[IP] Datagram with destination address of <destination address> cannot be forwarded
[IP] Reason: Invalid Device Info. Device <device name> is not IP callable
These two message appear together if a user calls in to the specified destination user and that user is not configured to be IP callable.

[IP] Default Route not added, invalid next hop (<IP address #>)
Because of an incorrect setup, the default route entry was not added in the routing table. Check the next hop in your configuration. Be sure that the next hop indicated by the <IP address #> is directly connected to the configured network interface.

[IP] Failed to de-register with IP Address Pool Manager (erc=x)
A failure was encountered by the IP subsystem during initialization processing. IP made an unsuccessful attempt to de-register as a provider of “static” addresses for the IP address pool. Contact your Distributor or Customer Support.

[IP] Failed to register with IP Address Pool Manager (erc=x)
A failure was encountered by the IP subsystem during initialization processing. IP made an unsuccessful attempt to register as a provider of “static” addresses for the IP address pool. Contact your Distributor or Customer Support.

[IP] Initialization failure
The IP Router was not initialized correctly because of other errors. Possible errors include “[IP] Cannot get system memory for xxxx”. Refer to the log for additional messages to pinpoint the problem.

[IP] Invalid configuration for Network Interface dd
IP routing is not properly configured. Refer to the *IP Network Interfaces* section to verify.

[IP] Invalid RLAN IP Address <IP address>, RLAN IP Stream Closed
The connection from a HDLC Bridge or a PPP device came up and the IP (sub-) network number configured for it is invalid; it does not belong to any of the WAN (RLAN) interfaces. Correct the IP address for the remote device.

[IP] Invalid Peer IP Address <IP address>, WAN IP Stream Closed
A PPP or RFC 1294 (IP Host) connection came up, and the IP address of the peer device (pre-configured or negotiated) belongs to a WAN (RLAN) Interface. If the IP address is preconfigured, try changing the peer's IP address (at the peer device and possibly on the device entry for the peer) that belongs to one of the WAN, WAN (Direct Host), or WAN (UnNumbered) interfaces. If the IP address is negotiated, try changing the IP address pool, or make sure that you really do want to use a WAN (RLAN) Interface.

[IP] IP host is initialized successfully
This message is posted when the system IP Host feature has initialized successfully.

[IP] IP router is initialized successfully
This message is posted when the system IP Router feature has initialized successfully.

[IP] Network initialized successfully on ddd.ddd.ddd.ddd
This message is posted when the numbered interface is successfully initialized on the indicated IP address.

[IP] Network Interface on LAN port <port #> already exists
There is another network interface that is configured for the LAN port indicated, and it was already initialized successfully. This means that there are multiple network interfaces configured for the same LAN port. You should correct the system configuration.

[IP] Network Interface on LAN port <port #> not initialized
The network interface for the LAN port indicated was not initialized because there is no Ethernet resource configured, or the Ethernet resource that is configured does not have the corresponding port. You should correct the system configuration.

[IP] Route (<IP address #1>) not added, invalid next hop (<IP address #2>)
The static route entry indicated by the <IP address #1> was not added in the routing table because the next hop indicated by the <IP address #2> is not located on any network directly connected to the configured network interface.

IPSec - Duplicate SA, Final Dest Addr: nn.nn.nn.nn SPI nn.nn.nn.nn
A Security Association with the same SPI and Final Destination Address already exists. If there is no SPI parameter listed, the Security Association table has been filled.

IPSec Security Associations initialized successfully

[IP] WAN (Direct Host) Interface for LAN port <port #> already exists
There is another WAN (Direct Host) type interface that is configured for the LAN port indicated, and it was already initialized successfully. This means that there are multiple WAN (Direct Host) type interfaces configured for the same LAN port. Use CFGEDIT to specify primary or secondary interface.

[IP] WAN (Direct Host) Interface <WAN interface name>, invalid associated LAN interface <LAN interface name>
The WAN (Direct Host) type interface could not come up; the associated LAN network interface, specified by configuration, was not found. Use CFGEDIT to delete old WAN (Direct Host) interface. Check for associated LAN interface, and add if necessary. Then add back the WAN (Direct Host) interface.

[IP] WAN (Direct Host) Interface for network <network #> on LAN port <port #> initialized successfully
This message is posted when WAN (Direct Host) interface for the indicated network is initialized successfully.

[IPCP] Invalid pre-configured IP address <IP address> for <device name>, ignored
There is a configured IP address for the remote device in the Device Table, but the IP address does not belong to any configured WAN interfaces. Check the configuration. You will most likely need to add another WAN interface.

[IPCP] IP Address Pool - Out of IP addresses
IPCP needed to allocate an IP address from the IP address pool, but there were no IP addresses available in the IP address pool. You may need to add more IP addresses to the pool.

[IPCP] Option Negotiation Failure, Non-Convergence detected
IPCP is terminated because an agreement could not be reached on the details of protocol. Refer to the specific documentation for the device in question to determine if it is configured correctly. Then, contact your Distributor or Customer Support.

[IPCP] Remote device does not negotiate IP address
Please configure IP address for the device <device name>
The IP address for the remote device is either improperly configured, or not configured at all. Check configuration and adjust.

[IPFILT] Filter "abcd" does not exist, ignored by application point "xyz"
This particular error message detects that an attempt has been made to apply a non-existent filter. In theory, this can only happen if someone manually modifies a configuration file (other than through CFGEDIT or Manage Mode).

[IP Host] Call Dropped: ID Response was not received from remote
The system did not receive a valid identification exchange from the remote IP Host. The system has rejected the incoming call. Refer to the *Quick Start* for proper setup of your particular device.

[IP Host] Call Dropped: XID was not received from remote
The system did not receive a valid identification exchange from the remote IP Host. The system has rejected the incoming call. Refer to the *Quick Start*.

[IP Host] Security Rejection - Digit string wrong length
The system did not receive a valid identification exchange from the remote IP Host. The Identification digit string from the remote device was not of an appropriate length. This string must be a 24 character string of ASCII digits (0-9), which is blank padded. The system has rejected the incoming call.

[IP Host] Security Rejection - Invalid Security ID <Id string>
The system has received an IP Host Id, <Id string>, from a remote device that is not configured in the Device List. The system has rejected the incoming call. Verify that the IP Host ID in the Device List information is identical to the IP Host Id configured in the remote device.

[IP Host] Security Rejection - Security ID cannot be validated with Authentication Server
The System authentication type is configured to obtain device information off-node, for example from a RADIUS server; however, such transactions are not yet supported when IP Host ID Security is enabled.

[IP RIP] All network interfaces used
All RIP interface data structures are in use. No RIP information will be sent to any additional interfaces. Contact your Distributor or Customer Support.

[IP RIP] Buffers allocated
The RIP successfully allocated the UDP buffers needed to transmit RIP packets.

[IP RIP] Initialization failed, unable to allocate buffers
The RIP initialization was not completed. The machine contains insufficient memory to allocate the UDP buffers needed to transmit RIP packets. Contact your Distributor or Customer Support.

[IP RIP] RIP Protocol Initialization successful
The RIP protocol was successfully initialized.

[IP RIP] Route Maintenance Registration Failed
The IP RIP protocol was unable to register with the IP routing table notification system. Any dynamic changes of the routing table configuration will not be reflected in the RIP packets sent to other routes. contact your Distributor or Customer Support.

[IP RIP] Send queue full
The RIP transmission queue has become full. This is not a normal occurrence. The machine should be restarted. If this message is displayed again after the machine has been restarted, contact your Distributor or Customer Support.

[IP RIP] Shutdown complete
The RIP protocol was successfully shutdown via Dynamic Management. No RIP routing information will be transmitted or received. Any routes learned via RIP will soon expire.

[IP RIP] Unable to add host route <IP address>
A failed attempt was made to add the host route to the IP RIP routing table. The routing table can have approximately 300 routing entries, and at this time, the routing table is full. The host route will not be broadcast via RIP packets and therefore other routers will not be able to learn the route to this device. You can use the packet capture commands to try to determine if a device is advertising an unusual number of routes. If you are unable to track down the problem, contact your Distributor or Customer Support.

[IP RIP] Unable to add route, routing table full
The IP RIP routing table is currently full, no new routes can be added. The routing table can have approximately 300 routing entries, and at this time, the routing table is full. This could result in possible unreachable destinations. You can use the packet capture commands to try to determine if a device is advertising an unusual number of routes. If you are unable to track down the problem, contact your Distributor or Customer Support.

[IP RIP] Unable to open RIP/UDP port 520
The UDP port for RIP was unable to be opened. There are 63 possible UDP ports, and none are available for use at this time. No RIP information can be transmitted or received. Contact your Distributor or Customer Support.

[IP RIP] Unable to register WAN Connection notification
The IP RIP protocol was unable to register with the IP WAN interface connection notification system. No WAN connection information will be reflected in the RIP packets. Contact your Distributor or Customer Support.

[IP RIP] Unable to register with Network Interface Maintenance
The IP RIP protocol was unable to register with the IP network interface notification system. Any dynamic changes of the network interface configuration will not be reflected in the RIP interface control. Contact your Distributor or Customer Support.

[IPX] Invalid IPXWC passed
In the unlikely event this message is posted, contact your Distributor or Customer Support.

[IPX] Network initialized successfully on xxxxxxxx:xxxxxxxxxxxx
This message is posted when the numbered interface is successfully initialized on the indicated IPX address.

[IPX] Network Interface on LAN port <port #> not initialized
The network interface for the LAN port indicated was not initialized because there is no Ethernet resource configured, or the Ethernet resource that is configured does not have the corresponding port. You should correct the system configuration.

[IPX] Route <IPX network address #1> not added: invalid next hop(<IPX address #2>
The static route entry indicated by the <IPX network address #1> was not added in the IPX routing table because the next hop indicated by the <IPX address #2> is not located on any network directly connected to the configured network interface.

[IPX] Route (<IPX network address>) not added: invalid next hop (<name>)
The static route entry indicated by the <IPX network address> was not added in the IPX routing table because the next hop remote device indicated by the <name> does not exist.

[IPX] IPX router initialized successfully
This message is posted when the IPX Router feature has initialized successfully.

IPX spoofing unable to get disconnect time structure. Default options replacing disconnect time options for device <device name>.
The resources required to properly perform the configured IPX spoofing options for the specified device after a connection to this device has been disconnected could not be obtained. The default IPX spoofing options are being used in place of the disconnect time IPX spoofing options.

[IPX RIP] Buffers allocated
The IPX RIP successfully allocated the buffers needed to transmit IPX RIP packets.

[IPX RIP] RIP Protocol Initialization successful
The IPX RIP protocol was successfully initialized.

[IPX RIP] Shutdown complete.
The IPX RIP protocol was successfully shutdown via Dynamic Management. No IPX RIP routing information will be transmitted or received. Any routes learned via IPX RIP will soon expire.

[IPX RIP] Space available in routing table
A route entry has become available in the full route table.

[IPX RIP] Unable to add route, routing table full
The route table has become full. The maximum number of route entries should be increased. Note: This message will not recur in the log until space becomes available in the route table.

[IPX SAP] Buffers allocated
The IPX SAP successfully allocated the buffers needed to transmit IPX SAP packets.

[IPX SAP] SAP Protocol Initialization successful
The IPX SAP protocol was successfully initialized.

[IPX SAP] Shutdown complete
The IPX SAP protocol was successfully shutdown via Dynamic Management. No IPX SAP service information will be transmitted or received. Any services learned via IPX SAP will soon expire.

[IPX SAP] Space available in service table
A service entry has become available in the full service table.

[IPX SAP] Unable to add service, service table full
The service table has become full. The maximum number of service entries should be increased.
Note: This message will not recur in the log until space becomes available in the service table.

[IPXCP] Add Network Address to Pool with value above <network address>
This message informs the administrator that negotiation was not possible since non-convergence was detected the network address sent by the peer was not acceptable by us and we do not have any network address to assign to the peer. The possible remedy is to configure more IPX addresses with a value more than <Network Address> in the Address Pool.

[IPXCP] IPX Address Match.
[IPXCP] Device <device> address same as another device address
The remote device indicated by <device> requested to use an already existing IPX network number and node number.

[IPXCP] Our Node Address is <node address>
This message informs the administrator that the peer has assigned us a node number because the system did not have a node address and the peer needs a node address. This node address will be used by the peer to identify this system.

[IPXWAN] Master Slave Conflict. Change Internal Network Number above <present value>
This message indicates that over the IPXWAN link, the master and slave roles could not be determined. The internal network number of the system must be changed to ensure proper IPXWAN negotiation to occur.

[IPXWAN] IPX Internal Network Number must be configured.
You must configure a valid internal network number in order for IPX routing to work properly.

L3_CallRefSelect Call Reference wrapped
Status message indicating that Layer 3's call reference value has wrapped. If this message is posted frequently, report the problem.

LAN Adapter Abort
The Ethernet adapter or subsystem is being interrupted as part of the error recovery process. If the system fails to operate normally, or the warning continues to occur, then report the event using the problem reporting form included in *Getting Assistance*.

LAN Adapter Command Timeout
The system expected a command from the LAN adapter or subsystem that it did not receive. Check for proper LAN adapter configuration and hardware installation. If it persists, report the event using the problem reporting form included in *Getting Assistance.*

LAN Adapter configuration conflict
There is a configuration conflict between the Ethernet resource that was installed and the Ethernet resource that was configured. Correct the configuration to match the installation.

LAN Adapter Fatal Error Reported
LAN Adapter hardware failure detected. If the problem persists, replace your LAN adapter.

LAN Adapter FIFO Data Underrun
The system expected data from the adapter that it did not receive, and the system will continue to operate. Check for proper LAN adapter configuration and hardware installation.

LAN Adapter FIFO not empty, status=<status value>
The LAN adapter did not enter the proper state after it was restarted. Check for proper LAN adapter configuration and hardware installation.

LAN Adapter HW upgrade may be required
Older versions of the Ethernet adapter may need to be updated to run Release 2.3 or greater. If the above message appears in your system log messages, you will need to remove your Ethernet adapter to determine if it is a version that needs to be updated. Refer to the "Notes and Warnings" section of the Release Notes for further instructions.

LAN Adapter HW upgrade required
Older versions of the Ethernet adapter may need to be updated to run Release 2.3 or greater. If the above message appears in your system log messages, you will need to upgrade your Ethernet adapter.

LAN Adapter LAN Controller error
The system detected an error with the LAN controller. The LAN adapter card may be faulty. Contact your Distributor or Customer Support.

LAN Adapter not configured
The system tried to access the bridging function when it was not configured. Most likely, the Ethernet resource was accidentally deleted. Correct the system configuration to reflect the proper Ethernet resource.

LAN Adapter out of receive buffers for LAN port <port #>
The LAN adapter is temporarily out of receive buffers for the indicated port. This condition should clear itself. If the condition persists, contact your Distributor or Customer Support.

LAN Adapter out of receive buffers for the WAN port
The LAN adapter is temporarily out of the buffers it uses to receive packets from the WAN port. This condition should clear itself. If the condition persists, contact your Distributor or Customer Support.

LAN Adapter port <port #> transmit error <error code>, check connection
The LAN adapter detected an error transmitting a frame on the indicated port. Check that the LAN is properly connected to the adapter and that the LAN is properly terminated.

LAN Adapter Reset
This is an initialization message. The Ethernet adapter has been reset as part of the adapter initialization sequence.

LAN Adapter Response Timeout
The system expected a command response from the adapter that it did not receive. Check for proper hardware installation.

LAN Adapter ROM version ########.########.########
The ROM version in the Ethernet adapter is indicated.

LAN Adapter software version conflict
When software is downloaded onto the Ethernet adapter, its software version is compared to the version of software running on the host's main processor. If the versions do not match, this message is posted. The upgrade did not work properly; contact your Distributor or Customer Support.

LAN Adapter System resource error
LAN Adapter hardware failure detected. If the problem persists, replace your LAN adapter.

LAN Init Error
LAN connection failure. Initialization failure detected by the LAN packet forwarding component in the system.

LAN Port <port #> detected a transceiver problem
The system detected a LAN connection problem on the indicated port. Check for proper LAN connection installation.

LAN Port <port #> detected jabber condition <n> times(s)
A "jabber" condition or an Ethernet frame larger than the maximum legal length has been received. This message is usually displayed if there is a malfunctioning transceiver or a malfunctioning Ethernet device on the LAN. This message is not displayed for every error condition. It appears after 24 hours since the last message was displayed. This message provides the LAN port # in question, and the number of times <n> the jabber condition has been detected.

LAN Port <port #> detected open LAN media
The system detected a problem with the physical LAN on the indicated port. The LAN is not properly terminated or the LAN is not fully connected to the system. Check for proper LAN installation.

LAN Port <port #> detected shorted LAN media
The system detected a problem with the physical LAN on the indicated port. The LAN is not properly terminated or the LAN is not fully connected to the system. Check for proper LAN installation.

LAN Port <port #> is now in the Forwarding state
The bridge LAN port indicated has entered the forwarding state and is now ready for data transfer.

LAN Port <port #> is now in the Learning state
The bridge LAN port indicated has entered the specified state.

LAN Port is now in the Listening state
The bridge LAN port is entering the specified state.

LAN Port <port #> is now in the <new state> state
The bridge LAN port indicated is entering the specified new state.

LAN Xmit Error
LAN connection failure. LAN packet transmit error detected by the system.

Layer 1 sync not seen - Slot=<slot #> Port=<port#> Ces=<communication endpoint suffix
A physical problem has been detected on the indicated line. Check for proper connection to the CyberSWITCH and to the NT1 or CIU. If the NT1 or CIU appears functioning properly, call your phone company and report the problem.

[LCP] Option Negotiation Failure, Non-Convergence detected
Link Control Protocol is terminated because the CyberSWITCH and the device cannot agree on a common way of communicating. The device may not be configured properly. Refer to the specific documentation for device set up. Then, contact your Distributor or Customer Support.

Line <slot #, port #> Down
ISDN line failure. The data link for the line connected to slot <slot #> port <port #> is down.

LMI alarm on Access <access index>
Indicates that either no STATUS messages have been received from the network or that N393 errors have occurred in the last N391 events thus exceeding the device configured alarm threshold for the LMI link. Any associated PVCs are disabled. (The variable N393 is the configured Monitored Events Count, and the variable N391 is the configured Full Status Enquiry Polling Count.)

LMI alarm reset Access <access index>
Indicates that N392 events have occurred which allows the LMI alarm condition to be cleared and any associated PVCs to be re-enabled. (The variable N392 is the configured Error Threshold Count.)

Loop detected on Local Area Network
The LAN adapter has detected a loop condition on the local area network. The system will discard these frames until the loop condition is removed.

MAC Layer Bridge did not Initialize
A system problem prevented the MAC layer bridge from properly initializing, and the bridge will not forward data over the WAN. Restart the system. If the error continues, contact your Distributor or Customer Support.

Manage Mode updates have been successfully committed
The above message indicates that the Dynamic Management commit command was successfully completed.

Manual intervention required: please replace LAN card
Older versions of the Ethernet adapter may need to be updated or replaced to run Release 2.3 or greater. If the above message appears in your system log messages, you will need to replace your Ethernet adapter.

Manual restart initiated on DM board in slot <slot #>
There was an attempt to restart the specified Digital Modem with the `modem restart` command. Check subsequent log messages to verify the command was successful.

Max ATI3 retries exceeded on modem <modem #> of slot <slot #>
Modem <modem #> in slot <slot #> did not respond to the proper modem revision string on power up. Call Customer Support.

Maximum call charges exceeded for month
The configured maximum for monthly call charges has been exceeded.

Maximum call minutes per day limit (x) has been reached
The described limit has been exceeded. The next log message will indicate whether calls will still be allowed or not.

Maximum call minutes per month limit (x) has been reached
The described limit has been exceeded. The next log message will indicate whether calls will still be allowed or not.

Maximum calls per day limit (x) has been reached
The described limit has been exceeded. The next log message will indicate whether calls will still be allowed or not.

Maximum calls per month limit (x) has been reached
The described limit has been exceeded. The next log message will indicate whether calls will still be allowed or not.

MCP detected channel failure: <channel number>
A link has failed for some abnormal reason and the indicated channel has been disconnected. This message is generally preceded by another message which indicates the underlying protocol. Refer to that message. If this does not pinpoint the problem, check the application on the remote device to see if it is working correctly.

Memory Access Timeout
This indicates a TDM bus connector failure that is specific to the TDM bus connecting a primary rate and a basic rate adapter. Ensure that the TDM bus has been correctly connected to the two adapters. If problem continues, contact your Distributor or Customer Support.

MEMORY LIMITED - <x> COMPRESSION connections available
Where "x" is equal to the number of connections that can be supported. There is not enough memory available to support the number of compression connections being allocated. You may want to purchase more memory for your system. Contact your Distributor or Customer Support.

Mild congestion CLLM received for DLCI <dlci index>
A CLLM message was received indicating mild congestion may be expected on the PVC associated with the indicated DLCI.

Mismatch of configured and installed DM card in slot <slot #>
The switch and / or jumper settings on the specified Digital Modem card are not properly set to match how the card is configured in software. Check the hardware and software configuration and restart.

Missing BEARER_CAPABILITY in HOST_CALL_REQUEST
Missing CALLED_NUMBER_IE in HOST_CALL_REQUEST
Missing CHANNEL in HOST_CALL_REQUEST
Missing CHANNEL_ID_IE in HOST_CALL_REQUEST
Missing TN in HOST_CALL_REQUEST
An error has been detected in the R2 or RBS signaling procedure, and will typically result in a failed call. The error was due to unrecognizable or incorrect information. Check configuration; if problem persists, contact your Distributor or Customer Support.

MODEM <modem #> of DM card in slot <slot #> is unusable
An attempt was made to perform an operation on a specific modem that had been deleted from the usable list via the *modem delete* command. Use the `modem add` command to make the modem usable again, or use a different modem to perform the desired operation.

MODEM CONNECT failed - connect <connect id #>, board <board #>, modem <modem #>
An attempted modem call has failed to connect. Try reconnecting the call again. If this message consistently appears for the same modem number, contact your distributor or Customer Support.

Modem revision on modem <modem #> of slot <slot #> failed
Individual modems on a Digital Modem card are failing. Check the hardware and software configurations, as well as the seating of the card and the MVIP cabling. If all seems in order, contact your Distributor or Customer Support.

Modem version comparison failed in slot <slot #> due to inconsistent format
This message displays if any of the following files are corrupted: DM56MDM.MOT, DM56PPCU.MOT, DM24MDMU.MOT, DM24PPCU.MOT. Contact your Distributor or Customer Support.

Negotiation Failure with Semipermanent device "x"
There was some problem negotiating a connection with device "x." There was no way to send data. This could be an authentication failure or a PPP failure.

Network loop between site1 and site 2
The system detected a WAN loop between the specified sites, so the System will not forward the duplicate frame. Check the System and network configuration for this loop and adjust.

Network requested init but no SPID configured- Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix>
A SPID is required but is not configured on the indicated line. The configuration of the CyberSWITCH or of the switch should be corrected.

Network sent bad Endpoint identifier - Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix>
During terminal initialization, a bad endpoint identifier was received on the indicated line. This message is informational only; your line should continue to operate normally.

Network sent CAUSE - invalid SPID - Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix>
An invalid SPID is configured on the indicated line. The configuration of the CyberSWITCH or of the switch should be corrected.

Network sent Cause - SPID not supported - <slot #, port #>
The indicated line does not support SPIDs; however, a SPID is configured for use on the line. Is the SPID configured incorrectly? Do you have the right switch type? Check the configuration. If the message persists, contact your BRI provider to determine corrective action.

Network sent STATUS with state = 0, tear down call
A STATUS message has been received from the network indicating that a specified call is not active. The system is removing the call.

No Active Calls
0 Active Sites
Currently, no sites are connected to the system.

No Active List entry available in INM
The system tried to contact a remote site and no table entries were available. You may need a larger version of the CyberSWITCH.

No CCB found, Port=<port #>, CallRef=<call reference #>
Contact your Distributor or Customer Support. Provide your distributor with a copy of the message log, and the output of the `wan stats` command. With the `wan stats` command, the main item of interest is the "rcv fail" number on the connections line.

No compression sessions are available due to memory constraints.
Check available memory; upgrade to a 12Mb system (minimum). If you are still encountering problems, disable unused protocols, and / or contact your Distributor or Customer Support to reduce your number of available connections.

NO FR LMI transmit buffer available
Indicates that, temporarily, no transmit buffer was available for formatting and sending a STATUS ENQUIRY message to the network.

NO FR LMI transmit buffer descriptor available
Indicates that, temporarily, no transmit buffer descriptor was available for control and administration of a STATUS ENQUIRY message to be sent to the network.

No internal b channel resources available, disconnecting call
The call is up, but there are no resources available to send the data. Contact your Distributor or Customer Support.

No resources available to accept incoming call
The System received an incoming call, but it had already established the maximum number of calls. This indicates the demand for network resources exceeds the configuration of this system. If this type of occurrence continues, you should consider upgrading to a larger system.

No response received from caller to our callback request. Terminating Call.
A modem connection negotiated callback, the CyberSWITCH sent a callback request to the caller (the PC) but got no response. Make sure the caller entered a callback phone number when prompted by the pop up screen.

No response to TEI requests - Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix>
TEI configuration mismatch between the system and the switch for the indicated line. The configuration of the system or of the switch should be corrected.

No Sites Connected
Currently, no sites are connected to the system.

Not enough memory for Security module
Not enough system memory available to operate security module. Contact your Distributor or Customer Support.

No UA seen in response to SABMEs - Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix>
Layer 2 cannot be established between the system and the switch. This could be a TEI configuration mismatch between the system and the switch for the indicated line. Check the configuration of the system. If this is not the problem, call your carrier. The configuration of the switch may need correction, or the line may need to be manually restarted.

No VCB buffer available
Ran out of sending buffers for messages to Combinet. If this is a recurring problem, contact your Distributor or Customer Support.

Number of optional connections reduced from xx to yy due to memory limitations
This informational message identifies that there is not enough memory available to accommodate the system's total capacity load for optional connections.

Number of required connections reduced from xx to yy due to memory limitations
This informational message identifies that there is not enough memory available to accommodate the system's total capacity load for required connections.

Offnode server lookup of Dial Out User failed.
Off-node authentication was not successful. Most likely, the device attempting to authenticate was not configured. Check configuration.

OSW <OSWFileName>, found in the Flash File System. The OSW has not been updated from this file due to insufficient Flash File System space. Please delete unnecessary files from the system.
Delete unneeded files to free up Flash File System space, and reboot the system. DO NOT DELETE NEX.BIN, IOP.BIN, OR UPGRADE.BIN. The system will again attempt to install the compressed file set after the system is rebooted again.

Outgoing calls barred - Slot=<slot #> Port=<port #>
The system cannot place outgoing calls on the indicated line. The switch must be configured to handle circuit switched data calls. Contact your phone company and report the problem.

Out of accounting records
Contact your Distributor or Customer Support.

Out of CCBs, Port=<port #>, CallRef=<call reference #>
Contact your Distributor or Customer Support.

Out of LAN Adapter transmit command descriptors
The LAN adapter is temporarily out of buffers used to transmit frames on to the Ethernet. This condition should clear. If it persists, contact your Distributor or Customer Support.

Out of overflow RAM buffers
Contact your Distributor or Customer Support.

Out Svc # <slot #, port #>
ISDN line failure. The line connected to the indicated slot and port is out of service for the reason indicated by #.

1 = No layer 1 sync for 5 seconds
This problem normally occurs due to WAN cabling problems.
Check your cables to make sure they are connected correctly. If this problem still occurs after you have checked all the cables, call the phone company and report the problem.

2 = No response to TEI requests
This problem normally occurs due to invalid configuration.
Check your configuration using the following table:

basic rate	*line from phone co: point-to-point*	*line from phone co: multi-point*
line configured on non-auto TEI	make sure that the configured TEI value is 0	change TEI to be AUTO
line configured on auto TEI	change TEI to be non-auto	if problem happens for over 5 minutes, report problem to phone company

3 = No UA response to SABME requests; no Layer 2
This problem normally occurs due to invalid configuration.
Check your configuration using the previous table.

4 = Failure to negotiate SPID (U.S. only). This is due to an improperly configured SPID. Check your configuration.

5 = Failure to negotiate SPID (U.S. only). SPID has not been configured on the system; check configuration.

Over Max Charge
Monthly call charges exceeded. Monthly call charge tracking is enabled and the configured maximum has been exceeded.

[PAP] Identification timeout on remote device
The remote device did not send the PAP Authenticate-Request packet within a required amount of time. Try again. If this persists, contact your remote site.

[PAP] Invalid password for <name> given by remote device
The system received the PAP Authentication-Request packet with the incorrect password for the device name <name>.

[PAP] Remote device did not respond to the request
The system sent PAP Authenticate-Request packets the maximum number of times, but the remote device did not send either Authenticate-Ack or Authenticate-Nak packets. The remote device may

not be working properly. Check the configuration of the remote device and reboot. If the problem recurs, contact your Distributor or Customer Support.

[PAP] Remote device rejected System Information <error message>
The system received the PAP Authenticate-Nak packet with the error message <error message> against the previous PAP Authenticate-Request sent by the system. The <error message> is from the remote device, and is device-specific. Contact the remote site for assistance.

[PAP] Unknown name <name> given by remote device
The system received the PAP Authenticate-Request packet with the unknown device name <name>.

Post <number>, HDLC #<number> External Loopback Test FAILED
The indicated HDLC controller, 80532 Device, failed an internal register test. The boot process should continue; however, make note of the error message in the event of a future problem.

Post <number>, HDLC #<number> Internal Loopback Test FAILED
The indicated HDLC controller, 80532 Device, failed an internal loopback test. The boot process should continue; however, make note of the error message in the event of a future problem.

Post <number>, HDLC #<number> Interrupt Test FAILED
The indicated HDLC controller, 80532 Device, failed an internal interrupt test. The boot process should continue; however, make note of the error message in the event of a future problem.

Post <number>, HDLC #<number> Register Test FAILED
The indicated HDLC controller, 80532 Device, failed an internal register test. The boot process should continue; however, make note of the error message in the event of a future problem.

Post <number>, HDLC #<number> Test FAILED
The indicated HDLC controller, 80532 Device, failed one of the constituent POSTs. The boot process should continue; however, make note of the error message in the event of a future problem.

Post <number>, ISDN Test FAILED
The specified D-channel controller, one of 4 2086 devices, did not pass its POST. The boot process should continue; however, make note of the error message in the event of a future problem.

Post <number> memory read error at <address>, expected <value>, read <value>
The specified memory POST failed at the specified address, with both the expected and actual memory values displayed. The boot process should continue; however, make note of the error message in the event of a future problem.

Post <number> NVRAM Failure
The non-volatile RAM failed during its POST. The boot process should continue; however, make note of the error message in the event of a future problem.

Post <number>, timed out waiting for i960 to respond during POSTs
The i960 failed to respond during the allotted amount of time during the specified POST. This is an i960 failure. The boot process should continue; however, make note of the error message in the event of a future problem.

[PPP] Link Failure Detected: No response to periodic Echo-Requests.
This message is logged by the feature when it detects a failed link.

PVC for DLCI <dlci index> not ACTIVE
A frame was received on the PVC associated with the indicated DLCI which was not active. This is a temporary condition, and results from an asynchronous operation between the network and customer-premise equipment regarding the state of the individual PVCs. If this problem persists, contact your Distributor or Customer Support.

PVC not allocated for <dlci index>
The frame relay software received a frame from the network on PVC using the indicated DLCI which has not yet been configured. It is likely that there is a configuration mismatch between nodes in the network such that a node is transmitting data to the node logging this error via a valid but as yet unallocated PVC.

PVC rcv wait q already full
Indicates a lack of system resources to handle the level of traffic being experienced. Contact your Distributor or Customer Support.

RADIUS authentication is not available. You must first ENABLE RADIUS user level authentication.
An attempt was made to configure the Terminal Server Security for RADIUS and RADIUS was not configured on the CyberSWITCH.

R2: Clearing chan <xx> due to abnormal forward reception
R2: Memory Slip Overflow Detected
R2: CLEAR_BACKWARD timed out on chan <xx>
R2: Transmit Overflow Detected
These messages may result in dropped calls. They indicate that the line may be extremely noisy, or that the modem installed in the system is not configured correctly (A-law vs. mu-law). Check configuration before proceeding.

R2: Illegal <event description>...
R2: Received unknown <primitive/message>...
R2: Unable to send host <specific request>...
These illegal events typically result in a failed call. Contact your Distributor or Customer Support.

R2: Task unable to allocate Scheduling Timer. Shutting down task.
R2: Unable to restart Scheduling Timer.
These are non-recoverable conditions in the R2 system. Most likely, an attempt was made to install R2 signaling on a system that does not support it. Contact your Distributor or Customer Support.

R2 not capable of Multichannel or Non-circuit calls
This illegal event typically results in a failed call. Contact your Distributor or Customer Support.

RBS: Channel <channel #> - Backing off of channel, GLARE detected.
An incoming and outgoing call occurred on the indicated channel at roughly the same time. The system discontinued the outgoing call in order to allow the incoming call to be established.

RBS: Encountered unknown source ID.
RBS_out_SM<channel #>: NO Dial Digits supplied.
RBS: Received unknown primitive from CC.
RBS: Received unknown primitive from L1.
RBS: Received unknown primitive from ME.
RBS: Received unknown primitive from RBS.
The above Robbed Bit Signaling messages indicate that the system software sent a message to the RBS state machine that the state machine was unable to recognize or the information was incorrect. If this message is displayed in the log messages, contact your Distributor or Customer Support.

RBS: LIF_AddTimer failure.
An event occurred that the RBS task interpreted as a call signaling event, but layer 1 is not properly initialized. Ensure that an ISDN line is not plugged into a RBS card.

RBS: LIF_GetBuffer failure.
RBS: Unable to send host CALL_CLEARED.
RBS: Unable to send host CALL_CONNECTED.
RBS: Unable to send host CALL_REQUEST_ACK.
RBS: Unable to send host HOST_CALL_INDICATION.
RBS: Unable to send host REMOTE_DISCONNECT
RBS: Unable to send package to host.
The above Robbed Bit Signaling messages indicate that the WAN card is not communicating properly with the host, probably due to a card failure. Contact your Distributor or Customer Support.

RBS_out_SM<channel #>: Timeout waiting for WINK.
The system went off-hook and the switch never "winked" back, going off-hook for a specified amount of time and then returning to on-hook. The switch must wink back in order to tell the system to start dialing. Contact the telephone company and ensure that the line is configured for wink-start.

RBS: Unexpected event chan = <channel #>, state = <state ID>
An illegal signaling event occurred in the RBS task on the specified channel. Ensure that the line is configured correctly and that it is using the expected RBS protocol. Excess noise on the line may also cause this event.

Read 0 bytes from file <file name> for WAN card in slot <slot #>
If seen repeatedly, the above message indicates a problem with your hard drive. Contact your Distributor or Customer Support.

Ready for XModem Download - <ESC> to abort
The user has requested an attempt to UPDATE the system software, or it was not possible to Boot the system the last time it was attempted.

Reattempting to Install File Set into Flash Memory
The SSB is re-attempting to install the FileSet. The Flash File System may have been corrupted when attempting to install the FileSet the first time. In the meantime, the Flash File System has been formatted.

Rebooting...
The system is going to wait until the WatchDog timer expires, which causes the entire system to reboot.

Received charge amount - <charge amount>
The system has received an advice of charge from the network for the call just disconnected. The charge for this call is indicated in the charge amount parameter.

Received CLLM while PVC for DLCI <dlci index> in unexpected state <state>
A CLLM message was received indicating that a network condition should be expected for the PVC associated with the indicated DLCI. However, this PVC is in the indicated state and as such is already acting on a previous network condition notification.

Remote peer ID discrepancy
The On-node Device Table and the remote end of the connection disagree on the identity of the remote end. Check configuration, and then reboot the remote device. If problem persists, contact your Distributor or Customer Support.

Replace Lithium Battery: Contact your Representative
If this message is displayed in the log messages, contact your Distributor or Customer Support before you power off your system.

Requested channel not available - <slot #, port #>
The system has attempted a call using a channel on the indicated line that was not available. The call will be retried over a different line if possible.

Reserved signal
This message is informational only and is used to indicate additional details on the <signal value> received in the "call progress" information message.

Resmem_gettotal: Enabled size <size>, greater than Checksize <size> for <sub name>
Internal error that should be reported to Customer Support.

ResMem_Malloc failure for subsystem <sub name>
(size=<size>, type=<type>, class=<class>, ra=<hex return address>)
ResMem_Malloc Size <size> too large for subsystem <sub name> (type=<type>, class=<class>
ra=<hex return address>)
ResMem_Malloc Device not registered (ra=<hex return address>)
ResMem_Obtainable Device not registered (ra=<hex return address>)
Any of the above three messages indicate that an internal error has occurred that should be reported to Customer Support. The system will restart when this error occurs.

Retrying download of DM card in slot <slot#> in <x> seconds
The system has failed on previous attempts to initialize the Digital Modem card. The system will retry a specific number of times before logging a failure message. Check the hardware and software configuration, reseat the card in its ISA slot, and / or check the MVIP cabling. If the problem persists, contact your Distributor or Customer Support.

Rx Channel Inactivity Detected
No keep-alive frames have been received over an active connection to a remote system. This indicates that the connection or the remote node has failed (or been powered-off) without an indication of the failure from the network. If the event continues, contact your Distributor or Customer Support.

Security Rejection - Bridge Address Security cannot use Authentication Server
Both options (Bridge Address Security and off-node User Authentication) are not supported simultaneously.

Security Rejection - Caller did not negotiate security
Bridge Security is configured. A caller attempted to send device data before (or without) negotiating the Bridge Address security.

Security Rejection - HDLC not supported by the caller
A properly formed Bridge Security negotiation packet was received but the remote bridge indicated that it did not support the HDLC protocol.

Security Rejection - Invalid Calling Line Id - <CLID>
The calling line identifier has not been configured for any valid device in the system Device list. The number <CLID> indicates the actual number presented by the network.

Security Rejection - Invalid Password (<password>) given
A properly formed Bridge Security negotiation packet was received. The bridge is registered in the System Device table and a password was provided, but the password provided did not match the password in the System Device table.

Security Rejection - No Bridge Address given by caller
A normal Bridge Security negotiation packet was received, but did not contain a bridge address. Check configuration. If problem persists, contact your Distributor or Customer Support.

Security Rejection - No Password given by caller
A properly formed Bridge Security negotiation packet was received, and the bridge is registered in the system Device Table, but a password is required and none was provided by the calling bridge. Check configuration. If problem persists, contact your Distributor or Customer Support.

Security Rejection - No Protocol List supplied
A Combinet has attempted to connect to the system without the required Protocol List information. Check configuration, and then reboot the Combinet. If problem persists, contact your Distributor or Customer Support.

Security Rejection - Timeout on Startup Complete
After a normal Bridge Security negotiation packet is received, and the System sends a response message, there is a five second time limit in which a “Startup Complete” message must be received. The above security rejection message is seen if the Startup Complete message is not received before the timer expires. Check to see if the response message was received by the calling bridge.

Security Rejection - Unknown Calling Bridge - <bridge address>
A properly formed Bridge Security negotiation packet was received but the bridge address is not registered in the system Device Table.

SemiPermanent. Local authentication failure of Semipermanent device "x"
The system failed to authenticate the indicated device. The semipermanent connection will be disabled. Compare the authentication device information configured on the system with the actual configuration of the remote device. Make corrections as needed. Then, issue the `call device <device name>` command to reinstate the semipermanent connection.

Semipermanent. Device "x" disconnected by admin
The administrator has issued a `disc device <device name>` command. Therefore, the system will not attempt to call the indicated device again. Issuing the `call device <device name>` command will make device "x" semipermanent again.

Semipermanent. Device "x" has a smaller Initial Data Rate than Base Data Rate. No connection made.
The semipermanent feature will make enough calls to meet but not exceed the device's Initial Data Rate. In this case, the Base Data Rate (normally 56 or 64 Kbps) is larger than the device's Initial Data Rate. The semipermanent feature cannot make any calls, or it will exceed the Initial Data Rate. Reconfigure your data rates.

Semipermanent. Device "x" has had "y" bandwidth drops within "z" seconds. This device is considered to have failed remote authentication.
Because the local system cannot always be aware of remote authentication failures, and because there is no way to recognize remote authentication failures in the system once the remote end is authenticated, the semipermanent feature will try to determine them by detecting excessive remote bandwidth drops. The remote device must drop a call 10 times within a 10 minute period to trigger this event.

> *Will try again in "w" minutes.*
> This will be displayed directly beneath the above message if a Session Interval is configured for the device.

Semipermanent. Device "x" reconnected by admin.
The administrator has issued the `call device <device name>` command after issuing the `disc device <device name>` command. This restarts the semipermanent feature for the indicated device.

Severe congestion CLLM received for DLCI <dlci index>
A CLLM message was received indicating severe congestion may be expected on the PVC associated with the indicated DLCI.

Signal for unknown CallCmd task: <task Id>
Contact your Distributor or Customer Support.

SIG_notify Failure. Called Session is not Active.
An error has been detected in the R2 signaling procedure, and will typically result in a failed call. The error was due to unrecognizable or incorrect information. If problem persists, contact your Distributor or Customer Support.

<slot #, port #> Cfg Error
Line vs. adapter configuration error. A line is configured for port <port #> that does not exist on the adapter in slot <slot #>.

[SNMP] Authentication failure, improper access rights
There are two possible causes for this message:

- The SNMP Agent received a SetRequest PDU that contained a Community Name with an MIB access level of MIB GUEST or MIB USER. The MIB access level must be MIB ADMIN to perform a SetRequest. The request was discarded.
- The SNMP Agent received a PDU that contained a Community Name with an MIB access level of MIB GUEST and an object Id that cannot be accessed with an MIB GUEST access level. The request was discarded.

[SNMP] Authentication failure, unknown community name
The SNMP Agent received a request PDU whose community name is not configured in the Community Names Table. The request was discarded.

[SNMP] SNMP initialization failure - unable to allocate necessary memory
The SNMP feature was unable to initialize because it could not obtain the necessary memory. The SNMP feature is disabled and no SNMP request will be processed. Contact your Distributor or Customer Support.

[SNMP] SNMP initialization failure - unable to open UDP port
The SNMP feature was unable to initialize because it could not obtain the necessary UDP port. The SNMP feature is disabled and no SNMP request will be processed. Check the configuration, and then contact your Distributor or Customer Support.

[SNMP] SNMP initialized successfully
The SNMP Agent has been successfully initialized and is fully operational.

[SNMP] Unable to obtain an SNMP Trap queue entry buffer
The SNMP Agent attempted to generate a TRAP PDU but was unsuccessful because it could not obtain necessary memory. The TRAP was not sent. Contact your Distributor or Customer Support.

[SNMP] Unable to obtain an SNMP Trap queue header
The SNMP Agent attempted to generate a TRAP PDU but was unsuccessful because it could not obtain necessary memory. The TRAP was not sent. Contact your Distributor or Customer Support.

SPID FSM got unidentifiable INFO msg - Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix>
An unexpected information message was received from the network on the indicated line. If you are having trouble establishing calls on this line, the problem should be reported to your phone company.

SSB: Can't read RTC prior to i960 POSTs
The Real Time Clock became inaccessible before invoking the i960 POSTs. The RTC is used to guard against infinite loops while waiting for the i960 to run its POST tests. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Couldn't read RTC during i960 POSTs
The Real Time Clock became inaccessible during the running of the i960 POSTs. The RTC is used to guard against infinite loops while waiting for the i960 to run its POST tests. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: i960 I/O memory copy differs from flash image at <address>
After loading the i960 POST tests into the I/O memory, a value unexpectedly changed at the address given.

SSB: i960 Memory read error at <address>, expected <value>, read <value>
While testing the shared memory area (I/O memory and the peripheral buffer memory), an error was detected. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: i960 POST number not equal to i386's
The i386 requested the i960 to run a specific POST. Upon receiving the response, from the i960, it was determined that a different POST was actually run.
The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 23 i960host_int_reg FAILURE
The i960 failed its internal register test. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 24 i960io_int_reg FAILURE
The i960 failed its I/O register test. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 25 i960io_mod_mem_1 FAILURE
The i960 failed its I/O memory test using the first test pattern. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 26 i960io_mod_mem_2 FAILURE
The i960 failed its I/O memory test using the second test pattern. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 27 i960timer_82c54FAILURE
The i960 failed its timer unit test. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 28 i960lan_82596sx FAILURE
The i960 failed its LAN Coprocessor test. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 29 i960lan_82503 FAILURE
The i960 failed its LAN transceiver test. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 30 i960per_mod_mem_1 FAILURE
The i960 failed its peripheral buffer memory test using the first test pattern. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 31 i960per_mod_mem_2 FAILURE
The i960 failed its peripheral buffer memory test using the second test pattern. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 32 i960hdlc_1 FAILURE
The i960 failed its 80532 test using the first HDLC controller. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 33 i960hdlc_2 FAILURE
The i960 failed its 80532 test using the second HDLC controller. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 34 i960hdlc_3 FAILURE
The i960 failed its 80532 test using the third HDLC controller. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 35 i960hdlc_4 FAILURE
The i960 failed its 80532 test using the fourth HDLC controller. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 36 i960isdn_1 FAILURE
SSB: Post 37 i960isdn_2 FAILURE
SSB: Post 38 i960isdn_3 FAILURE
SSB: Post 39 i960isdn_4 FAILURE
The i960 failed its 2086 test using the first (second, third or fourth) D-channel controller The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Timed out waiting for i960 to initialize for POSTSs
The i960 did not respond to an initialization request in a timely manner. This is a i960 failure. The boot process should continue; however, make note of the error message in the event of a future problem.

Starting Triggered RIP/SAP for <device>
This message indicates that triggered RIP / SAP has started for a device (either locally configured or one present in the WAN peer list). Triggered RIP / SAP has been configured as a routing protocol for this particular device.

Stream Ready rejected - MTU too small
The remote device will only accept the stream connection if the MTU is set to be $\geq$ 1514. Check to make sure that the remote device and the CyberSWITCH MTU value is set to $\geq$ 1514.

[STP] A BLAN Topology Change has been detected
The system has detected a topology change in the Spanning Tree environment.

[STP] A new Root Bridge has been detected
The system has detected a new root bridge for the Spanning Tree environment.

[STP] LAN Port <port #> is now a Designated Port
The indicated LAN port has become the designated port for the attached LAN.

[STP] LAN Port <port #> is now the Root Port
The indicated LAN port has become the root port for the system.

[STP] This Bridge is now the Root Bridge
The system has become the root bridge for the Spanning Tree environment.

Successfully Loaded Release <X.Y> Issue <Z>
The specified release of System software was successfully loaded into memory.

Switch could not recognize phone number nnnnnnn
The switch did not accept the phone number dialed as a complete number. Check the correctness of the phone number (including any leading digits such as 8 or 9).

System Clock Fault on Wan Adapter in Slot <slot #>
Indicates a TDM bus connection failure. Check to make sure that the TDM bus has been correctly connected.

TACACS authentication is not available. You must first ENABLE TACACS user level authentication.
An attempt was made to configure the Terminal Server Security for TACACS and TACACS was not configured on the CyberSWITCH.

TCP Connection to CSM at <IP address> is DOWN; reason: <reason code>.
The TCP connection to the Connection Services Manager (CSM) has gone down. Contact your Distributor or Customer Support and provide them with the indicated reason code.

TCP Connection to CSM at <IP address> is UP.
A TCP connection exists between this device and the CSM at the indicated IP address.

TCP Connection to CSM Lost.
The TCP connection to the CSM has gone down.

TDM Clock Master changed TO (slot #, port#) FROM (slot #, port #)
The Clock Manager has dynamically adjusted the master clock source in response to an external line state change.

Temporarily unable to read flash file system due to flash reclaim in progress - try again later
The system is automatically performing a flash reclaim to reclaim space previously occupied by deleted files. Wait several seconds (up to a minute maximum) and try your file system command again.

Terminal Server Security connections disabled. Dropping call.
The Terminal Server Security is set to *none* and a terminal connection was requested. Check configuration. Most likely, the Default Async Protocol is set to terminal with no Terminal Server Security configured.

Terminal Server Security is currently using this database. You must change the Terminal Server Security setting first.
An attempt was made to disable a User Level Security Database when the terminal server was configured to use this database for terminal mode authentication.

[TFTP] Data buffer allocated successfully
All parts of the TFTP feature (both Server and Client) were successfully initialized.

Note: The following "[TFTP] Local error..." messages generated during client operations will be displayed on the console only and will not be logged to disk.

[TFTP] Local error #2: Feature not initialized
The TFTP feature was not initialized properly. No file transfer will be attempted. Check the configuration, and then contact your Distributor or Customer Support.

[TFTP] Local error #3: Server not initialized
The TFTP Server was not initialized. The TFTP Server will not attempt any file transfers. Check the configuration, and then contact your Distributor or Customer Support.

[TFTP] Local error #4: UDP rejected packet <filename>
The UDP subsystem could not send the data because there was a problem with the file. If this message appears consistently, contact your Distributor or Customer Support.

[TFTP] Local error #5: UDP open failed
The UDP subsystem could not open a new port. No file transfer will be attempted. Check the configuration, and then contact your Distributor or Customer Support.

[TFTP] Local error #6: All UDP buffers in use <filename>
All of the TFTP / UDP buffers are in use. There may be a problem with the specified file; try replacing it. If this message appears consistently, contact your Distributor or Customer Support.

[TFTP] Local error #7: Received packet with size zero
The TFTP protocol received a packet with no data.

[TFTP] Local error #8: No route defined <filename>
The TFTP protocol was instructed to start a TFTP session with an IP ADDRESS (HOST) for which there is no defined route. There may be a problem with the specified file; try replacing it. If this message appears consistently, contact your Distributor or Customer Support.

[TFTP] Local error #9: File transfer timed out <filename>
The TFTP file transfer timed out. There may be a problem with the specified file; try replacing it. If this message appears consistently, contact your Distributor or Customer Support.

[TFTP] Local error #10: IP addressing inconsistency detected
The TFTP protocol received a packet from a host for which no file transfer was being processed. This should not affect any files being transferred.

[TFTP] Local error #11: Received packets out of sequence <filename>
The TFTP protocol received a data packet that either was too old or one was skipped. There may be a problem with the specified file; try replacing it. If this message appears consistently, contact your Distributor or Customer Support.

[TFTP] Local error #12: Bad packet length received <filename>
The TFTP protocol received a packet that was too big. There may be a problem with the specified file; try replacing it. If this message appears consistently, contact your Distributor or Customer Support.

[TFTP] Local error #13: Received unexpected opcode <filename>
The TFTP protocol received a packet that was not expected. There may be a problem with the specified file; try replacing it. If this message appears consistently, contact your Distributor or Customer Support.

[TFTP] Local error #14: Bad file name
The local file (as defined from a remote host) was not recognized as a valid file name. No file transfer will be attempted.

[TFTP] Local error #15: Bad mode string
The TFTP mode string was not NETASCII nor OCTET. No file transfer will be attempted.

[TFTP] Local error #17: Unable to locate file/directory <filename>
The file system was unable to locate the file requested. No file transfer will be attempted.

[TFTP] Local error #18: Unable to open file <filename>
Either the file does not exist or the device (Client or Server) does not currently have access to this file. No file transfer will be attempted.

[TFTP] Local error #19: Disk full <filename>
The local disk became full during the TFTP file transfer. There may be a problem with the specified file; try replacing it. If this message appears consistently, contact your Distributor or Customer Support.

[TFTP] Local error #20: Error while writing file <filename>
An error occurred while writing to a file. The file may be corrupted and must be replaced.

[TFTP] Local warning #21 All sessions in use
All of the allowed TFTP sessions are currently in use. No file transfer will be attempted. (TFTP client console message only; not logged on System.)

[TFTP] Local warning #22 Feature Disabled
The TFTP feature was disabled from within Dynamic Management's Manage Mode. (TFTP client console message only; not logged on System.)

[TFTP] Local warning #23 Server Disabled
The TFTP Server was disabled from within Dynamic Management's Manage Mode. (TFTP client console message only; not logged on System.)

[TFTP] Local warning #24 Client Disabled
The TFTP Client was disabled from within Dynamic Management's Manage Mode. (TFTP client console message only; not logged on System.)

[TFTP] Local warning #26 TFTP Session Killed
The TFTP session was terminated by the network administrator via issuing the *`TFTP kill <session Id>`* console command.

Note: For the following [TFTP] Remote error messages the Remote Host TFTP Servers/Client will map error messages within the types shown below. The text portion of each message may vary with each Host transmitting the message.

[TFTP] Remote error #0: (Text from Remote Host)
Undefined error. The accompanying text (if any) should describe the error. The file being transferred may be corrupted.

[TFTP] Remote error #1: (Text from Remote Host)
The REMOTE HOST could not find the file specified on its system. No file transfer will be attempted.

[TFTP] Remote error #2: (Text from Remote Host)
The REMOTE HOST is reporting an access violation of the specified file. No file transfer will be attempted.

[TFTP] Remote error #3: (Text from Remote Host)
The REMOTE HOST is reporting that its disk is full. The file being transferred may be corrupted.

[TFTP] Remote error #4: (Text from Remote Host)
The REMOTE HOST is reporting that it received a TFTP packet that it was not expecting. The file being transferred may be corrupted.

[TFTP] Remote error #5: (Text from Remote Host)
The REMOTE HOST is reporting that it was not expecting a packet from our system. The file being transferred may be corrupted.

[TFTP] Remote error #6: (Text from Remote Host)
The REMOTE HOST is unable to overwrite the specified file. No file transfer will be attempted.

[TFTP] Remote error #7: (Text from Remote Host)
This message indicates that the specified device does not exist. This error should not occur since TFTP does not use Device Ids.

[TFTP} Server UDP port (69) closed successfully
Informational message stating that the TFTP server UDP port was successfully closed.

[TFTP} Server UDP port (69) opened successfully
Informational message stating that the TFTP server UDP port was successfully opened.

[TFTP] Unable to allocate data buffers
The entire TFTP feature (both Server and Client) was not initialized. Contact your Distributor or Customer Support.

[TFTP] Unable to open Server UDP port (69)
The TFTP Server was not initialized; however, the TFTP Client may still work. If this message occurs repeatedly, or if the TFTP Client does not work, contact your Distributor or Customer Support.

The call deflection selection is prior to CCITT 1988
Verify that the facilities provided by the service provider are CCITT 1988.

The call has been disconnected
A call has been up longer than the amount of time configured and has been taken down.

The call is allowed to continue
A call has been up longer than the amount of time configured, but it has not been taken down.

The compression subsystem is not enabled
Check CFGEDIT; verify that compression is enabled.

The conformance selection is prior to CCITT 1988
Verify that the facilities provided by the service provider are CCITT 1988.

The RADIAC Feature is no longer supported. The RADIAC feature has been replaced by the TACACS Feature. The TACACS Feature configuration must be completed before usage.
With the addition of User Level Security, the need for the RADIAC GATEWAY is gone. The CyberSWITCH has incorporated the functionality of the RADIAC GATEWAY within the CyberSWITCH itself. When the configuration file parser encounters a system configured for using the RADIAC feature, it switches the configuration to now use User Level Security utilizing a TACACS off-node authentication server. Since the older CyberSWITCH knew nothing about the location of the TACACS server, the TACACS server configuration must be completed before the CyberSWITCH will allow network access through a WAN connection.

The tone signaling state machine detected an invalid modem revision #
Current modem firmware may not be capable of proper tone signaling. You may need to upgrade your modem firmware. Contact your Distributor or Customer Support.

This card does not support R2 Signaling.
For R2 support, you will need a PRI-23/30 and a DM-24+ or DM-30+. Verify configuration. If you need to upgrade, contact your Distributor or Customer Support.

Timeout detected on connection establishment
The system initiated a connection with a remote site, but a time-out occurred while waiting for a connection response from the network. Verify that the remote site is active and that the network is operational.

Timeout detected on receiving caller's number
The incoming call security feature is enabled and the caller's number was not received, so the call was disconnected. Contact your phone company and verify that your switch supports passing along the calling number information element. (This is sometimes referred to as ICLID for InComing Line Identification).

Timeout on SPID Exchange - Slot=<slot#> Port=<port #> Ces=<communication endpoint suffix>
SPID exchange was not completed in time (i.e., switch never responded to the SPID). Check switch configuration to make sure the correct SPID value has been entered.

Timeout on Startup Complete
A startup complete message was not return from the Combinet after we sent the response a number of times. Check the configuration, and then reboot the Combinet. If problem persists, contact your Distributor or Customer Support.

Timeout waiting for DL Config Response
Timeout waiting for DSL Config Response
Timeout waiting for Terminate DSL Response
The above messages indicate that an attempt has been made to dynamically update the Data Link configuration, but the system did not receive a response from a Basic Rate adapter for an earlier request. Restart the system and review the configuration for the adapter. If the problem persists, the indicated adapter card may be faulty. Contact your Distributor or Customer Support.

Too many digits in TN in HOST_CALL_REQUEST
(R2 Signaling) This illegal event typically results in a failed call. Contact your Distributor or Customer Support.

Tried to free unallocated buffer <sub name>, size=<size>
Internal error that should be reported to Customer Support.

Transmit rate increased to <transmit rate>: Access <access index>, DLCI <dlci index>
The effective transmit rate has been increased to the indicated rate for the indicated DLCI under the indicated access.

Transmit rate reduced to CIR <transmit rate>: Access <access index>, DLCI <dlci index>
The effective transmit rate has been limited to the Committed Information Rate which is the rate for the indicated DLCI under the indicated access.

Type mismatch of configured & installed adapter #'x'
Configuration mismatch between the indicated adapter and the resource that was configured. The system resource configuration should be corrected.

Unable to add dynamically-obtained device data into Device Table
The System authentication type is configured to obtain device information off-node. If such information cannot be stored internally due to a temporary resource shortage, the call is dropped.

Unable to allocate IPX spoofing memory. IPX spoofing is being performed in a degraded mode.
The memory required by the IPX spoofing feature could not be allocated. The IPX spoofing code will continue to run but it will run in a degraded mode. The default IPX spoofing options will always be used when a connection is down to a device.

Unable to allocate port structure for port <port name> with address <AppleTalk Address>
Contact your Distributor or Customer Support.

Unable to allocate unnumbered wan port for device <device name>
Contact your Distributor or Customer Support.

Unable to complete Bridge Dial Out call: Insufficient information configured for Dial Out Device
Verify that *Bridging* and *Make Calls for Bridge Data* are enabled at the device level.

Unable to communicate with encryption board
Try again. If the problem persists, you may have a faulty encryption board. Replace the board.

Unable to Decrypt Datagram
An incoming datagram could not be decrypted. Verify encryption parameters on both nodes.

Unable to dynamically determine incoming call usage: Call Released.
This message refers to an incoming analog call which is going through the digital modem. The digital modem has transferred the call to the AUD to determine type of call. The AUD did not recognize any PPP LCP frames to transfer to the PPP stack, nor did it recognize the four carriage returns it requires (within 5 seconds of connection) for remote analog console access.

If you are attempting remote analog console access, be sure to press the carriage return four times within 5 seconds of making the connection.

Unable to get Digital Modem resource to place call
A Digital Modem dial-out call was attempted, and the system was unable to open a resource to place the call. Using the `modem status` command, check to ensure that there are usable modems available. If there are, and the problem persists, contact your Distributor or Customer Support.

Unable to Identify a remote device
A device that was not identified by any active security measures (for example, PAP or CHAP) was rejected.

Unable to Identify a remote device - <calling line id
A device that was not identified by any active security measures (for example, PAP or CHAP) was rejected and is identified by its Calling Line Id.

Unable to Identify a remote device - no CLID
A device that was not identified by any active security measures (for example, PAP or CHAP) was rejected and the caller did not present a Calling Line Id.

Unable to identify the frame type <CCB: xxxx>
The frame type (raw HDLC, RFC 1294, or PPP) can not be identified and therefore the connection has been terminated. "CCB: xxxx" is included for your Distributor or Customer Support. The most likely causes for the problem are: malfunction of the remote device, or a faulty line. Begin by checking the configuration of the remote device, and then rebooting the device. If this does not solve the problem, contact your Distributor. He/she will help you determine whether or not the line is faulty.

Unable to locate device entry in on-node database for terminal session
A device matching the login id entered at the user level security prompt was not found in the on-node database, and CSM was not configured.

Unable to open \config\devdb.nei file
Disregard this message if you have not yet added at least one device to the system's on-node device table and saved the change. The configuration file, \config\devdb.nei, is created the first time the device table is saved. If the message continues, contact your Distributor or Customer Support.

Unable to open file DM56MDM.MOT for Modem revision verification on slot <slot #>
The CyberSWITCH could not find the DM56MDM.MOT file in the C:\SYSTEM directory. Contact your Distributor or Customer Support.

Unable to open Modem Upgrade file
There may be a problem with the modem revision file. Contact your Distributor or Customer Support.

Unable to register WAN Connection notification
RADIUS Accounting is enabled, but IP is not enabled (and IP routing is required). Check for proper configuration in CFGEDIT. If the problem persists, contact your Distributor or Customer Support.

Unable to restore original ISRs for Interrupt <interrupt #>
Check hardware jumpers and switches on the DM card and reinstall. Verify that the DM card is properly configured in CFGEDIT. If the problem persists, contact your Distributor or Customer Support.

Unable to send device information request to CSM after a terminal authentication.
Unable to send information to CSM. Verify proper configuration of CSM and Call Control options.

Unable to send DL Config Request
Unable to send DSL Config Request
Unable to send Terminate DSL Request
The above three messages indicate that an attempt has been made to dynamically update the Data Link configuration, but the system is unable to send an update message down to a Basic Rate adapter. Restart the system and review the configuration for the adapter. If the problem persists, the indicated adapter card may be faulty. Contact your Distributor or Customer Support.

Unexpected error during transmission of LMI frame
A system error occurred during the actual transmit request for an LMI frame. Contact your Distributor or Customer Support.

Unknown Calling Bridge <MAC address>
MAC address security is enabled and the remote Combinet does not match any of the defined devices.

Unknown message type in SIG_get_rsc_inbound
Unknown message type in SIG_get_rsc_outbound
An error has been detected in the R2 signaling procedure, and will typically result in a failed call. The error was due to unrecognizable or incorrect information. If problem persists, contact your Distributor or Customer Support.

Unknown DLCI <dlci index> in CLLM message
The network has sent a CLLM message which has referenced the indicated DLCI that has not been configured. Check the system configuration for the indicated DLCI.

Unknown Security Association
An incoming datagram specifies a Security Parameter Index (SPI) which has not been defined on this node. Verify the encryption parameters on both nodes. Adjust if necessary so that both nodes reflect the same SPI.

Unmatched Login Task
This represents an internal system error. Contact your Distributor or Customer Support.

Unsupported Combinet protocol received: <protocol Id>
An unsupported Combinet protocol attempted to connect to the system. Contact your Distributor. You may need to upgrade software to support this.

Unsupported Combinet protocol version received: '<version Id>'. [Device: <device name>]
An unsupported Combinet version attempted to connect to the system. Contact your Distributor. You may need to upgrade software to support this.

Updating CyberSWITCH from "<FileName>"
The specified file, received during a Reliable Remote Upgrade, was successfully loaded into memory and will now be verified before installation into the Flash File System.

User Level Authentication flag is enabled for Terminal User xxx. Setting flag to disabled.

The device definition for xxx should have User Level Authentication disabled.
These two messages are displayed together. In device entries for terminal server connections, user-level authentication should not be enabled. In the event the CyberSWITCH finds an enabled condition, it will disable the pertinent flag for the duration of the call only. To avoid this situation permanently, disable the user level authentication flag in device entries for all terminal server connections.

Waiting for WAN card in slot <slot #> to complete initialization
Download process update for WAN card in slot <slot #>.

WAN card in slot <slot #> signals it is operational
Download process update that indicates that WAN card in slot <slot #> is now operational.

WAN Port is now in the Forwarding state
WAN port connections used by the bridge are now entering the specified state.

WAN Port is now in the <new state> state
The WAN connection port used by the bridge is entering the specified new state.

WAN: RBS Not Available on this card.
A RBS debugging command was attempted on a PRI card that is not configured for RBS. Check the card configuration and ensure you have the proper type of card.

WAN: Verbose Messaging Not Available on this card.
WAN: RBS Not Available on this card.
A RBS debugging command was attempted on a PRI card that is not configured for RBS. Check the card configuration and ensure you have the proper type of card.

Watchdog timeout detected on DM board in slot <slot #>
The Digital Modem card in the specified slot is not functioning properly. Check the board's configuration in CFGEDIT, reseat the board in its ISA slot, and check any MVIP bus cabling. If everything seems in order and the problem persists, contact your Distributor or Customer Support.

Watchdog timeout detected on WAN board 'x'
The system has detected that the indicated adapter has failed. This is a fatal condition and will cause the card to be reset. Verify the *settings* on the adapter. If theses are all correct and the problem persists, the indicated adapter card may be faulty. Contact your Distributor or Customer Support.

The following messages are reported when a remote X.25 device's facilities do not match with those configured locally:

X25 facilities error, facilities not allowed in PVC
A facility is configured, for example call deflection, which is not allowed in a PVC. Check your PVC configuration.

X25 facilities error, fast select with restriction on response was required
The fast select with restriction on response is required. Verify that fast select is enabled by both DTE's and the service provider.

X25 facilities error, bad facility length
The facilities length is missing. Contact your Distributor or Customer Support.

X25 facilities error, invalid facilities length
The length of the facilities packet is invalid. Contact your Distributor or Customer Support.

X25 facilities error, invalid DTE address
The supplied address in a X.25 call packet was invalid. Verify that the local DTE address configuration matches the address supplied by the service provider.

X25 facilities error, facility not allowed
A facility was requested which is not enabled. Verify that the specific facility is enabled by both DTE's and the service provider.

X25 facilities error, facility length too short
The length of the facilities packet is too short. Contact your Distributor or Customer Support.

X25 facilities error, invalid facilities parameter
A value was chosen for facility which is out of the acceptable range of values for that facility. The range of acceptable values for that facility should be verified at both DTE's and by the service provider.

X25 facilities error, reverse charging not allowed
The reverse charging facility was selected by the DTE. Verify that reverse charging is enabled by both DTE's and the service provider.

X25 facilities error, reverse charging not accepted
The reverse charging facility was selected by the DTE. Verify that reverse charging is enabled by both DTE's and the service provider.

X25 facilities error, fast select not available
The fast select facility was selected by the DTE. Verify that fast select is enabled by both DTE's and the service provider.

X25 facilities error, fast select not accepted
The fast select facility was selected by the DTE. Verify that fast select is enabled by both DTE's and the service provider.

X25 facilities error, throughput negotiation not allowed
The DTE throughput class does not match the throughput class available at either the DCE or the remote DTE, and throughput negotiation is not enabled. You should enable throughput negotiation at both DTE's. If this is not possible, or does not work, select the same throughput class at both DTE's.

X25 facilities error, closed device group not allowed
The closed device group facility was selected by the DTE. Verify that the closed device group facility is enabled by both DTE's and the service provider.

X25 facilities warning, reverse charging info not available
The service provider does provide reverse charging information. No action required.

X25 facilities error, facility not available
A facility was requested which is not enabled. Verify that the specific facility is enabled by both DTE's and the service provider.

X25 facilities error, packet length negotiation not allowed
The DTE packet length does not match the packet length available at either the DCE or the remote DTE, and packet length negotiation is not enabled. You should enable packet length negotiation at both DTE's. If this is not possible, or does not work, select the same packet length at both DTE's.

X25 facilities error, window size negotiation not available
The DTE window size does not match the window size available at either the DCE or the remote DTE, and window size negotiation is not enabled. You should enable window size negotiation at both DTE's. If this is not possible, or does not work, select the same window size at both DTE's.

X25 facilities error, RPOA not available
Recognized Private Operating Agency selection is not available. The System does not support this feature.

X25 facilities warning, transit delay not available
The service provider does provide transit delay information. No action required.

X25 facilities warning, charge inform not available
The service provider does provide charging information. No action required.

X25 facilities warning, call redirect notification not available
The service provider does provide call redirect information. No action required.

X25 facilities warning, NUI not available
Network device identification not available. No action required.

X25 permanent virtual circuit down: Access=<access index>, PVC=<PVC index>, LCN=<LCN>
The indicated X.25 virtual circuit is down. Switched backup connections will be used, if available. This message will occur if the other system is down, or if the network interface line is not connected, or if the authentication of the remote device failed.

X25 permanent virtual circuit to device <device name> up: Access=<access index>, PVC=<PVC index>, LCN=<LCN>
The indicated X.25 virtual circuit is operational.

XMODEM DATA FAILED CRC CHECKS
A file contained in the X-Modem file set has failed the CRC check. The system will automatically reset and attempt a reboot in an effort to correct the problem. If the system continues to fail, make note of the displayed messages, and call your distributor. A software update is likely needed.

Zone allocation failed, increase zone table capacity.
The number of AppleTalk zones has surpassed the configured zone table capacity. The CyberSWITCH configuration utility allows you to set the maximum number of defined and learned zone table entries. The default value is 512. The maximum is 2,000. You may need to reset the zone table capacity to a higher number.

Zone allocation failed, maximum capacity already configured
The maximum number of AppleTalk zones have been surpassed. Contact your Distributor or Customer Support.

TRACE MESSAGES

OVERVIEW

Trace messages include the following categories of messages:

1. Call Trace Messages
2. IP Filter Trace Messages
3. PPP Packet Trace Messages
4. WAN FR_IETF Trace Messages
5. X.25 Trace Messages
6. X.25 (LAPB) Trace Messages

Before trace messages can be logged to the system report log, you must first enable the type of trace you would like to use. Once enabled, the system includes the trace messages in the memory-resident report log. To access this log, use the following commands:

dr or *ds*	display reports or display statistics
er or *es*	erase current messages / statistics from memory
wr or *ws*	write reports / statistics to disk

When the system writes system messages to disk, it stores them in the following locations:

Directory:	`\log`
File Name:	`rprt_log.nn` (where "nn" is an integer that is incremented each time a new file is written.)

The system reports messages using the following format:

Message Type		Time	Report Number	Message
I	Informational	hour:minutes:second	internal ID for area reporting the message	actual text of the message
W	Warning			
E	Error			

Where:

- The Message Type quickly identifies the type of message the system reports.
- The Time identifies when the message was reported.
- The Report Number is used by your Distributor or Cabletron Customer Support.
- The Message text describes the actual message being reported.

Below, there is a separate section included for each category of trace messages. For each category, a definition of the trace message type, the command to enable / disable the logging of the trace messages, and an alphabetized list of the associated messages is included.

CALL TRACE MESSAGES

A feature of the CyberSWITCH console is the ability to save and display a record of the high level ISDN calls between the system and the local telephone switch. If calls are unable to be completed, this is normally the first area to look.

Call Trace puts messages into the Report log that can be read by using the *dr* command. Call Trace is enabled by using the *trace on* command, and disabled by *trace off*.

The following is a description of the possible fields included in a Call Trace Message:

1. The <Call Id> field in the message can be used to keep track of messages for the same phone call. This is useful when a system is making more than one call at a time.

2. The In-Disconnect and In-Information messages have a location field. This identifies where the message originated.

   The following chart provides a list of locations that may appear in Call Trace messages:

Location Causes	
Value	*Meaning*
0	remote device
1	private local network
2	public local network
3	transit network
4	private remote network
5	public remote network
7	international network
FF	local CyberSWITCH system

3. The In-Disconnect messages have a cause field. This is the value (in hex) that was in the message. It explains why either a call was disconnected or why a call attempt was not able to be completed. There are also parameters (such as <signal value>, <progress value>), that are not described here. These values represent messages reported from the switch. We have attempted to interpret their significance in the error message text itself.

   Refer to the *Cause Codes* table, for a complete listing of cause codes.

When the call trace option is enabled, the system may report messages such as:

```
(I)    13:55:46.98 #1067: Out - CALL RQST CallId=0x8000 Rate=64 Slot=1 Port=1
       Chans=0x2 TN=181 Ces=0 ConnId=0
(I)    13:55:46.98 #1063: In - CALL RQST ACK CallId=0x8000 Slot=1 Port=1
       Ces=1ConnId=0
(I)    13:55:47.43 #1063: In - PROCEEDING CallId=0x8000 Slot=1 Port=1 Chans=0x1
       Ces=1 ConnId=0
(I)    13:55:47.60 #1063: In - CONNECT Call_id=0x8000 Slot=1 Port=1 Chans=0x0
       Ces=1 ConnId=0
(I)    13:55:54.16 #4D11: LAN Port 1 is now in the FORWARDING state
```

CALL TRACE MESSAGE SUMMARY

Access information discarded cause
Call trace message. This message is used to indicate additional details on the <cause value> received in the "call progress" information message.

Alerting off
Informational call trace message. The alerting signal information element is off. This indicates additional details on the <signal value> received in the "call progress" information message.

Alerting on - pattern <pattern number>
Informational call trace message. This indicates additional details on the <signal value> received in the "call progress" information message.

Answer tone on
Informational call trace message. This message is used to indicate additional details on the <signal value> received in the "call progress" information message.

Call has returned to the ISDN
Informational call trace message.

Call is not end-to-end ISDN
One or more of the WAN phone networks used to connect the call is not an ISDN network. The call must be at 56 Kbps.

Call waiting tone on
Informational call trace message. It indicates additional details on the <signal value> received in the "call progress" information message.

Custom tone on
Informational call trace message.

Delay in response at called interface
Informational call trace message.

Destination call address is non-ISDN
Informational call trace message.

Dial tone on
Informational call trace message.

Disconnect for <tone value> tone on
This message indicates that the system disconnected the outbound call. The <tone value> values are: error tone, busy verify, confirm, busy, network congestion, or intercept. These tone values indicate a temporary network failure. Check the outbound phone number and try again. If the problem persists, contact your phone company.

Expensive routing tone on
Informational call trace message.

In - ABNORMAL RPT Call Id=<call Id> Slot=<slot #> Port=<port #> ConnId=<connect Id> Ces=<communication endpoint suffix>
The system has detected an internal error condition. The <parameters> are included for your Distributor or Cabletron Customer Support. An error message describing the problem should be reported following this trace message.

In - ABNORMAL RSP Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix> Err=<error> Sev=<severity> State=<state>
The system has detected an invalid internal message type. Contact your Distributor or Cabletron Customer Support. The <parameters> are included for your Distributor or Customer Support.

In - ALERTING Call Id=<call Id> Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix> ConnId=<connect Id> Chans=<bearer channel map>
Informational call trace message. The system has received an alerting message from the network. The Call Id and Ces values are included for your Distributor or Cabletron Customer Support. The remaining parameters are used to report line details.

Inband treatment has been applied
Call trace message (informational only). There are audible tones on the B-channel. (Refer to "Disconnect for <tone value>" message for possible tone values.) If the message persists, contact your Distributor or Cabletron Customer Support.

In -BRD CFG ACK Slot=<slot #>
This is an initialization acknowledgment message for the indicated adapter. It is in response to a configure message.

In - CALL RQST ACK Call Id=<call Id> Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix> ConnId=<connect Id>
A call request acknowledgment for the indicated call request.

In - CHAN STATUS Call Id=<call Id> Slot=<slot #> Port=<port #> Channel=<channel> Action=<action> ChanState=<channel state> SvcsState=<service state>
The system has received a channel status message from the network. This message is received when the status of a bearer channel on a line has changed. The <parameters> specify the channel and the new state.

In - CLEAR Call Id=<call Id> Slot=<slot #> Port=<port #> Loc=<location> Cause=<cause value> Ces=<communication endpoint suffix> ConnId=<connect Id>
The system has received a call clear message from the network. This is usually received after a call disconnect is either initiated by the system or the network. The <parameters> are included for your Distributor or Cabletron Customer Support. Refer to the *Cause Codes Table* for more information.

In - configure ack <slot #>
This is an initialization acknowledgment message for the indicated line adapter. It is in response to a configure message.

In - CONNECT Call Id=<call Id> Slot=<slot#> Port=<port #> Chans=<bearer channel map> Ces=<communication endpoint suffix> ConnId=<connect Id>
The system has received a connect message from the network. This indicates that a new call is now established and ready for use. The Call Id and Ces values are included for your Distributor or Cabletron Customer Support. The remaining parameters are used to report line details.

In - DISCONNECT Call Id=<call Id> Slot=<slot #> Port=<port #> Loc=<location> Cause=<cause value> Ces=<communication endpoint suffix> ConnId=<connect Id>
The system has received a disconnect message from the network. The Call Id and Ces values are for your Distributor or Cabletron Customer Support. The remaining parameters are used to report line details. Refer to the *Cause Codes Table* for more information.

In - DL CFG ACK Slot=<slot #> Port=< port #> Ces=<communication endpoint suffix
This is a data link initialization acknowledgment for the indicated data link.

In - DSL CFG ACK Slot=<slot #> Port=< port #>
This is a line initialization acknowledgment for the indicated line.

In - FACILITY ACK Call Id=<call Id> Slot=<slot #> Port=<port #> ConnId=<connect Id> Ces=<communication endpoint suffix>
The system has received a facility acknowledgment message from the network. The Call Id and Ces values are included for your Distributor or Cabletron Customer Support. The remaining parameters are used to report line details.

In - FACILITY Call Id=<call Id> Slot=<slot #> Port=<port #> ConnId=<connect Id> Ces=<communication endpoint suffix>
The system has received a facility message from the network. The Call Id and Ces values are included for your Distributor or Cabletron Customer Support. The remaining parameters are used to report line details.

In - FACILITY REJ Call Id=<call Id> Slot=<slot #> Port=<port #> Loc=<location> Cause=<cause> ConnId=<connect Id> Ces=<communication endpoint suffix>
The system has received a facility rejection message from the network. The Call Id and Ces values are included for your Distributor or Cabletron Customer Support. The remaining parameters are used to report line details. Refer to the *Cause Codes Table* for more information.

In - INCOMING CALL Call Id=<call Id> Slot =<slot #> Port=<port #> Chans=<bearer channel map> Ces=<communication endpoint suffix> Rate=<data rate>
The system has received an incoming call from the network. The system will respond with a connect or a disconnect message. The Call Id and Ces values are included for your Distributor or Cabletron Customer Support. The remaining parameters are used to report line details.

In - INFORMATION Call Id=<call Id> Slot=<slot #> Port=<port #> Chans=<bearer channel map> CauseLoc=<cause location> Cause=<cause value> Signal=<signal value> ProgLoc=<progress location> Prog=<progress value> Ces=<communication endpoint suffix> ConnId=<connect Id>
The system has received a call progress message from the network. This is usually received in response to sending a call request. The <parameters> are included for your Distributor or Cabletron Customer Support. Refer to the *Cause Codes Table* for more information.

In - init data link <slot #, port #, ces>
The WAN card in slot <slot#> attempted to initialize the data link for port <port#> with Communication Endpoint Suffix <ces>.

In - PROCEEDING Call Id=<call Id> Slot=<slot #> Port=<port #> Chans=<bearer channel map> Ces=<communication endpoint suffix> ConnId=< connect Id>
The system has received a call proceeding message from the network. This is usually received in response to sending a call request. The Call Id and Ces values are included for your Distributor or Cabletron Customer Support. The remaining parameters are used to report line details.

In - PROGRESS Call Id=<call Id> Slot=<slot #> Port=<port #> Chans=<bearer channel map> CauseLoc=<cause location> Cause=<cause value> Signal=<signal value> ProgLoc=<progress location> Prog=<progress value> Ces=<communication endpoint suffix> ConnId=<connect Id>
The system has received a call progress message from the network. This is usually received in response to sending a call request. The <parameters> are included for your Distributor or Cabletron Customer Support. Refer to the *Cause Codes Table* for more information.

In - REJECTION Call Id=<call Id> Slot=<slot #> Port=<port #> Loc=<location> Cause=<cause value> Ces=<communication endpoint suffix> ConnId=<connect Id>
The system has received a call rejection message from the network. This is in response to sending a call request. The Call Id and Ces values are included for your Distributor or Cabletron Customer Support. The remaining parameters are used to report line details. Refer to the *Cause Codes Table* for more information.

Interworking unspecified cause
Informational call trace message. This message is used to indicate additional details on the <cause value> received in the call progress information message. Refer to the *Cause Codes Table* for more information.

Off-hook warning tone on
Informational call trace message.

Origination call address is non-ISDN
Informational call trace message.

Out - ALERTING Call Id=<call Id> Slot=<slot #> Port=<port #> Chans=<bearer channel map>
The system is sending a connection to the network. This is sent in response to receiving a call indication. The <parameters> are included for your Distributor or Cabletron Customer Support.

Out - BRD CFG Slot=<slot #>
The system is initializing the indicated adapter.

Out - CALL RQST ACK Call Id=<call Id> Rate=<data rate> Slot=<slot #> Port=<port #> Chans=<bearer channel map> TN=<telephone number dialed> Ces=<communication endpoint suffix> ConnId=<connect Id>
The system is sending a call request to the network. The Call Id and Ces values are included for your Distributor or Cabletron Customer Support. The remaining parameters are used to report line details.

Out - configure <port #>
The system is initializing the indicated line adapter.

Out - CONNECT Call Id=<call Id> Slot=<slot #> Port=<port #> Chans=<bearer channel map> Ces=<communication endpoint suffix> ConnId=<connect Id>
The system is sending a connection to the network. This is sent in response to receiving a call indication. The <parameters> are included for your Distributor or Cabletron Customer Support.

Out - DISCONNECT Call Id=<call Id> Slot=<slot #> Port=<port #> Cause=<cause value> Ces=<communication endpoint suffix> ConnId=<connect Id>
The system is sending a disconnect to the network to terminate a call. The Call Id and Ces values are included for your Distributor or Cabletron Customer Support. The remaining parameters are used to report line details. Refer to the *Cause Codes Table* for more information.

Out - DL CFG Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix>
The system is initializing the indicated data link.

Out - DSL CFG Slot=<slot #> Port=<port #>
The system is initializing the indicated line.

Out - init data link <slot #, port #, ces>
The system is sending a message to the network to initialize a data link on an ISDN line. The <parameters> are used to report line details.

Out - PROCEEDING Call Id=<call Id> Slot=<slot #> Port=<port #> Chans=<bearer channel map> Ces=<communication endpoint suffix> ConnId=<connect Id>
The system is sending a connection to the network. This is sent in response to receiving a call indication. The <parameters> are included for your Distributor or Cabletron Customer Support.

Recall dial tone on
Informational call trace message.

Received charge amount - <charge amount>
The system has received an advice of charge from the network for the call just disconnected. The charge for this call is indicated in the charge amount parameter.

Received unknown abnormal report value Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix>
Informational call trace message.

Received unknown progress value
Informational call trace message.

Received unknown signal value
Informational call trace message.

Ringback tone on
Informational call trace message.

Status report progress value received
Informational call trace message.

Stutter tone on
Informational call trace message.

Tones off
Informational call trace message.

Unspecified cause
Informational call trace message. This message is used to indicate additional details on the <cause value> received in the "call progress" information message.Refer to the *Cause Codes Table* for more information.

Unspecified tone
Informational call trace message. It is used to indicate additional details on the <signal value> received in the "call progress" information message. The <tone value> is displayed as one of the following: dial, ring back, answer, call waiting, off hook warning, custom, recall dial, stutter dial, or expensive routing.

IP FILTERS TRACE MESSAGES

You can trace packets that are discarded as a result of IP Filters. Enable this feature by using the `ip filter trace discard` command, and disable it with `ip filter trace off`. Note that when you enable this feature, the report log has the potential of filling quickly. Use the feature wisely, and be sure to turn it off once you've completed your troubleshooting. Access the discarded packet information via the report log by using the `dr` command.

Each discarded packet will cause a log report of the following format:

(F) _:_:_:_:#9a00 [IPFILT] <filtername>/condition # at <application point name>/in/out
{IP} Src: xxx.xxx.xxx.xxx Dst: xxx.xxx.xxx.xxx Pr: n
{UDP} Src: n Dst: n

The first line indicates:

- the number of the condition within that filter which matched the packet and consequently caused a *discard* action,
- the point at which the filter was applied, or a designation of *global*. For an IP network interface, this will be the configured name of the interface. For a device-based filter, this will be the configured device's name.
- *In* or *Out*, corresponding to INPUT or OUTPUT application.

The next lines contain a brief decode of the packet which was discarded. In particular, the packet fields which comprise the packet type comparisons are displayed. The key IP fields are always displayed on one line. If the IP protocol is one of the explicitly recognized values (ICMP, UDP, TCP), the next line will contain a decode of the key fields of that protocol.

Sample IP Filter Trace Discard logs:

(I) 10:11:50.43 #9A00: [IPFILT] UDP/1 at Intf. lan/Out
(I) 10:11:50.43 #9A00: {IP} Src: 128.131.0.1 Dst: 128.131.0.7 Pr:17
(I) 10:11:50.43 #9A00: {UDP} Src: 5001 Dst: 69

- Filter *UDP*, condition 1, applied at interface *lan's OUTPUT*

(I) 10:11:50.71 #9A00: [IPFILT] ICMP/1 at Global
(I) 10:11:50.71 #9A00: {IP} Src: 0.0.0.0 Dst: 128.131.0.7 Pr:1
(I) 10:11:50.71 #9A00: {ICMP} Code: 8 Type: 0

- Filter *ICMP*, condition 1, applied *globally*

PPP PACKET TRACE MESSAGES

PPP Packet Trace allows you to display the PPP protocol negotiation that takes place when a link is established. This information is useful when diagnosing mismatches in configuration between two systems. PPP Packet Trace puts PPP packet information into the Report log, which can be accessed by using the *dr* command. Enable this feature by using the *trace ppp on* command, and disable it with *trace ppp off.* Two other commands are also available, *trace ppp np* and *trace ppp cp*. *trace ppp np* only enables the tracing of Network Protocol packets received and sent by the system. When the *trace ppp np* command is used, no Control Protocol packets will be reported to the system message log. *trace ppp cp* only enables the tracing of Control Protocol packets received and sent by the system. When the *trace ppp cp* command is used, no Network Protocol packets will be reported to the system message log.

The following is the format of a PPP trace line as it is displayed by *dr:*
[connection Id] [packet direction] [protocol type] [packet type]

where:

[connection Id]
Identifies the connection. The Id is a numerical value, allowing you to distinguish connections. The numerical value represents the order in which the connections are generated.

[packet direction]
Indicates the packet direction. IN means received packet, OUT means transmitted packet.

[protocol type]
Indicates the type of protocol used for negotiation. When a connection is made between two devices, there are three different phases. The last two phases deal with the protocol type and the options negotiated.

The following table summarizes the protocol types:

Protocol	*Options Negotiated*
Link Control Protocol	Authentication Protocol (PAP,CHAP) Multilink Protocol (MRRU, Endpoint Discriminator)
PAP CHAP	Password validation Shared Secret validation
Compression (CCP) Encryption (ECP) IPCP BCP IPXCP ATCP	Compression options Encryption options IP address Bridge options IPX options Appletalk options

[packet type]
A code field that indicates the type of command that the packet contains. PPP Control Protocol negotiation uses the following commands:

- *Configure Request*
  The Configure Request is used to indicate the options that are supported by this sending device. The Request contains an option list and the desired values if they are different from the default value.

- *Configure ACK*
  The Configure ACK is transmitted in response to a Configure Request. It indicates that the sending device supports the options specified in the option list of the Configure Request and that all values are acceptable. The receiving device assumes that negotiation is complete for the Control protocol being configured.

- *Configure NAK*
  The Configure NAK is transmitted in response to a Configure Request. It indicates that the sending device understands, but does not accept the values of the options specified in the option list of the Configure NAK. The option list of the NAK only contains the unacceptable options. The receiving device should choose different options and send another Configure Request with the new option list and values.

- *Configure Reject*
  The Configure Reject is transmitted in response to a Configure Request. It indicates that the sending device does not understand the options specified in the option list of the Configure Reject. The option list of the Reject only contains the unknown options. The receiving device must assume the sender cannot process the rejected options in any manner, and take appropriate action. The Configure Reject inherently provides backward compatibility with older PPP implementations.

- *Terminate Request*
  The Terminate Request is transmitted when a device wishes to close down the connection.

- *Terminate ACK*
  The Terminate ACK is sent in response to a Terminate Request and indicates that the sending device has closed the connection.

- *Code Reject*
  The Code Reject is transmitted by a device if it does not recognize the PPP command type received from the other device.

- *Protocol Reject*
  The Protocol Reject is transmitted by a device if it does not recognize the PPP protocol type received from the other device.

- *Echo Request*
  The Echo request is used to provide a Data Link layer loop back detection mechanism. The Echo Request packet contains the magic number of the sending device. Until the magic number option has been negotiated the value must be set to zero.

- *Echo Reply*
  The Echo Reply is transmitted in response to an Echo Request. The Echo Reply packet contains the magic number of the sending device. Until the magic number option has been negotiated the value must be set to zero.

- *Discard Request*
  The Discard request packet is transmitted by a device to exercise the data link layer processing. This packet is silently discarded by the receiving device.

WAN FR_IETF TRACE MESSAGES

You can trace Frame Relay (FR_IETF) incoming and outgoing packets. This FR_IETF trace information is placed into the Report log, which can be accessed by using the *dr* command. Enable this feature by using the *wan fr-ietf trace on* command, and disable it with *wan fr-ietf trace off*. You can specify the direction of the packets (*in* or *out*), a particular device or PVC (*<device>* or *<fr_accessname_dlci>*) and the protocol (*AT*, *BR*, *IP*, or *IPX*) to be traced.

The following is the format of a FR_IETF trace line as it is displayed by *dr*:
[packet direction]: [device name or fr_accessname_dlci] [protocol] size:[NN]

where:

[packet direction]
Indicates the packet direction. IN means received packet, OUT means transmitted packet.

[device name or fr_accesname_dlci]
Indicates the device or Frame Relay PVC associated with the traced data.

[protocol]
Identifies the protocol type of the traced data. Protocol types are AT (AppleTalk), BR (MAC Layer Bridge), IP, and IPX.

[NN]
Identifies the size of the data in bytes.

X.25 TRACE MESSAGES

It is now possible to trace X.25 incoming and outgoing packets. This X.25 trace information is placed into the Report log, which can be accessed by using the *dr* command. Enable this feature by using the *trace x25 on* command, and disable it with *trace x25 off*.

X.25 TRACE MESSAGE SUMMARY

In - X25 Call Connect LCN <logical channel number>, <number of bytes> bytes
The DTE has accepted an incoming SVC call.

In - X25 Clear Ind LCN <logical channel number>, <number of bytes> bytes
An SVC call has been cleared by the DCE.

In - X25 CONNECTION CONFIRMATION ConnId=<connection Id> Access=<access index> RemDteAddr=<x121 address or protocol/route id>
The system has received a connect message from the network. This indicates that a new call is now established.

In - X25 CONNECTION INDICATION ConnId=<connection Id> Access=<access index > RemDteAddr=<x121 address or protocol/route id>
The system has received an incoming call from the network. The system will respond with a connect or a disconnect message.

In - X25 DATA LCN <logical channel number>, <number of bytes> bytes
Data transfer.

In - X25 DCE Clear Conf LCN <logical channel number>, <number of bytes> bytes
The DCE is confirming that an SVC call has been cleared by the DTE.

In - X25 DCE Interrupt LCN <logical channel number>, <number of bytes> bytes
An interrupt packet has been received from the DCE. Flow control procedures do not apply to interrupt packets.

In - X25 DCE Intr Conf LCN <logical channel number>, <number of bytes> bytes
The DCE is confirming that an interrupt packet has been received.

In - X25 DCE REJ LCN <logical channel number>, <number of bytes> bytes
The DCE has detected a packet sequence error.

In - X25 DCE Restart Conf LCN <logical channel number>, <number of bytes> bytes
The DCE is confirming that all virtual circuits have been reset.

In - X25 DCE RNR LCN <logical channel number>, <number of bytes> bytes
The DCE is not ready to receive packets from the DTE.

In - X25 DCE RR LCN <logical channel number>, <number of bytes> bytes
The DCE is acknowledging data packets from the DTE.

In - X25 Diagnostic LCN <logical channel number>, <number of bytes> bytes
The DCE is providing a diagnostic packet with a cause and an error code.

In - X25 DISCONNECT CONFIRMA]TION Connid=<connection Id> Access=<access index>
The system has received a disconnect confirmation message from the network. This is usually received after a call disconnect is either initiated by the system or the network.

In - X25 DISCONNECT INDICATION ConnId=< connection Id > Access=< access index > Cause=<cause for disconnect> Diag=<diagnostic for disconnect>
The system has received a disconnect message from the network.

In - X25 Incoming LCN <logical channel number>, <number of bytes> bytes
An SVC call has been received from the DCE.

In - X25 Reset Ind LCN <logical channel number>, <number of bytes> bytes
The DCE is resetting a virtual circuit.

In - X25 Restart Ind LCN <logical channel number>, <number of bytes> bytes
The DCE is resetting all virtual circuits.

Out - X25 Call Accept LCN <logical channel number>, <number of bytes> bytes
The DTE is accepting an SVC call.

Out - X25 Call Request LCN <logical channel number>, <number of bytes> bytes
The DTE is attempting to place an SVC call.

Out - X25 Clear Ind LCN <logical channel number>, <number of bytes> bytes
The DCE is clearing the X.25 Virtual circuit on the indicated LCN.

Out - X25 Clear Request LCN <logical channel number>, <number of bytes> bytes
The DTE is clearing the SVC call on the indicated LCN.

Out - X25 CONNECTION REQUEST VcType=<virtual circuit type> ConnId=<connection Id> Access=<access index> RemDteAddr=<x121 address or protocol/route id>
The system is sending a call request to the network.

Out - X25 CONNECTION RESPONSE ConnId=<connection Id> Access=<access index>
The system is sending a connection to the network. This is sent in response to receiving a call indication.

Out - X25 DATA LCN <logical channel number>, <number of bytes> bytes
Data transfer.

Out - X25 DISCONNECT REQUEST ConnId=<connection Id> Access=<access index> Cause=<cause for disconnect>
The system is sending a disconnect to the network to terminate a call.

Out - X25 DISCONNECT RESPONSE ConnId=<connection Id> Access=<access index>
The system has received a disconnect response from the network.

Out - X25 DTE Clear Conf LCN <logical channel number>, <number of bytes> bytes
The DTE is confirming that the virtual circuit on the indicated LCN has been cleared.

Out - X25 DTE Interrupt LCN <logical channel number>, <number of bytes> bytes
An interrupt packet has been sent to the DCE. Flow control procedures do not apply to interrupt packets.

Out - X25 DTE Intr Conf LCN <logical channel number>, <number of bytes> bytes
The DTE is confirming the reception of an interrupt packet from the DCE.

Out - X25 DTE REJ LCN <logical channel number>, <number of bytes> bytes
The DTE has detected a packet sequence error.

Out - X25 DTE Reset Conf LCN <logical channel number>, <number of bytes> bytes
The DTE is confirming that the virtual circuit has been reset.

Out - X25 DTE Restart Conf LCN <logical channel number>, <number of bytes> bytes
The DTE is confirming that all virtual circuits have been reset.

Out - X25 DTE RNR LCN <logical channel number>, <number of bytes> bytes
The DTE is not ready to receive more data packets.

Out - X25 DTE RR LCN <logical channel number>, <number of bytes> bytes
The DTE is acknowledging 1 or more data packets received from the DCE.

Out - X25 Reset Ind LCN <logical channel number>, <number of bytes> bytes
The DCE is resetting a virtual circuit.

Out - X25 Reset Request LCN <logical channel number>, <number of bytes> bytes
The DTE is resetting a virtual circuit.

Out - X25 Restart Ind LCN <logical channel number>, <number of bytes> bytes
The DCE is resetting all virtual circuits.

Out - X25 Restart Req LCN <logical channel number>, <number of bytes> bytes
The DTE is resetting all virtual circuits.

X25 access <access index> in state <X25 manager state text> for event <X25 manager event text>
Tracks the X.25 access as it is coming up or going down, defining the state it is in and the event that is occurring.

X.25 (LAPB) TRACE MESSAGES

You can trace X.25 Link Access Procedure Balanced (LAPB) incoming and outgoing packets. This LAPB trace information is placed into the Report log, which can be accessed by using the `dr` command. Enable this feature by using the `trace lapb on` command, and disable it with `trace lapb off`.

X.25 (LAPB) TRACE MESSAGE SUMMARY

In - LAPB DISC
The DCE link layer is going off-line.

In - LAPB DM
The DCE is going off-line.

In - LAPB FRMR
The DCE has received an invalid frame.

In - LAPB I Frame, Tx Sequence = <sequence Id>, Rx Sequence = <sequence Id>
The DTE has received a data frame from the DCE.

In - LAPB REJ, Rx Sequence = <sequence Id>
The DCE has detected a sequence error in the link layer.

In - LAPB RNR, Rx Sequence = <sequence Id>
The DCE is not ready to receive more frames.

In - LAPB RR, Rx Sequence = <sequence Id>
The DCE is acknowledging one or more frames from the DTE.

In - LAPB SABM
The DCE is resetting the link layer.

In - LAPB SABME
The DCE is resetting the link layer.

In - LAPB UA
The DCE is acknowledging a SABM or SABME from the DTE.

Out - LAPB DISC
The DTE link layer is going off-line.

Out - LAPB DM
The DTE is going off-line.

Out - LAPB FRMR
The DTE has received an invalid frame.

Out - LAPB I Frame, Tx Sequence = <sequence Id>, Rx Sequence = <sequence Id>
The DTE has sent a data frame from the DCE.

Out - LAPB REJ, Rx Sequence = <sequence Id>
The DTE has detected a sequence error in the link layer.

Out - LAPB RNR, Rx Sequence = <sequence Id>
The DTE is not ready to receive more frames.

Out - LAPB RR, Rx Sequence = <sequence Id>
The DTE is acknowledging one or more frames from the DCE.

Out - LAPB SABM
The DTE is resetting the link layer.

Out - LAPB SABME
The DTE is resetting the link layer.

Out - LAPB UA
The DTE is acknowledging a SABM or SABME from the DCE.

SYSTEM MAINTENANCE

This grouping of information provides information to help you maintain your CyberSWITCH once it is operating. Note that the included system statistics information may also prove valuable in troubleshooting.

We include the following chapters in the *System Maintenance* segment of the *User's Guide*:

- *Remote Management*
  Once the CyberSWITCH is initially configured, you may use methods to remotely manage the CyberSWITCH. This chapter provides information for using each of these methods.

- *System Commands*
  A listing of all system console commands and associated command definitions.

- *System Statistics*
  A listing of all system statistics and associated statistic definitions.

- *Routine Maintenance*
  Instructions for performing routing CyberSWITCH maintenance.

REMOTE MANAGEMENT

OVERVIEW

Once your system is initially configured (and thus assigned an IP address), you may use a variety of methods to remotely access and manage your system. This chapter describes many of these methods.

For information on first-time access (either local or remote), refer to *Accessing the CyberSWITCH*.

The CyberSWITCH has various tools to manage the system remotely. You may combine several of these tools to provide a complete, customized remote network management system. In this chapter we will describe the tools, and explain several options to manage your system.

These tools are:

- SNMP (Simple Network Management Protocol)
- Telnet
- WIN95 Dial-up Networking
- TFTP (Trivial File Transfer Protocol)
- Carbon Copy

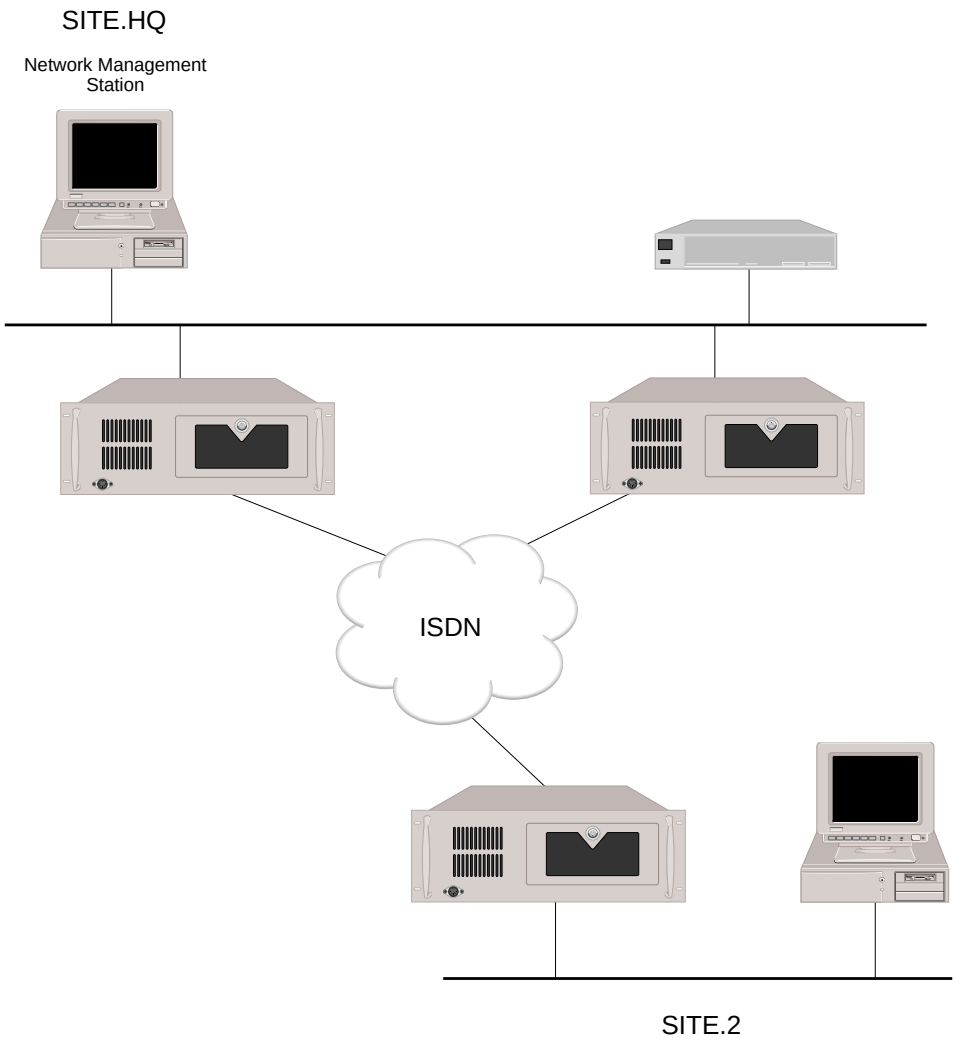
If the network is a bridged network, use the Carbon Copy utility for remote management. If the network is an IP network, use a combination of the remaining remote management tools.

Examples of usage in an IP network:

- SNMP can inform you of problems in the network as they occur.
- Telnet will allow you to issue console commands on a remote CyberSWITCH.
- TFTP can transfer report or statistics files from the CyberSWITCH, or new configuration files to/from the system.

A brief description of each tool follows.

SNMP



SNMP: The NMS gathers information (including problem reports) from any CyberSWITCH

SNMP (Simple Network Management Protocol) is a standard way of monitoring communication devices in IP networks. With SNMP, you purchase and then set up a Network Management Station (such as SPECTRUM® or SPECTRUM® Element Manager™) for your environment. This Network Management Station (NMS) is then used to monitor your network. From the NMS you can look at information from all the CyberSWITCHes and other remote devices. You can detect problems without manually check each machine to see if it is working correctly.

INSTALLATION AND CONFIGURATION

SNMP has two basic components: the *SNMP Agent*, which is executed on the CyberSWITCH, and the *Network Management Station (NMS)*, which you purchase separately for the environment. This section will describe how to install and configure the SNMP Agent. Refer to the specific NMS documentation for its installation instructions.

SNMP must be configured through CFGEDIT. Before configuring the SNMP Agent, you must have the following information:

- the Community Name(s) used in SNMP request messages generated by the NMS;
- the IP address of the NMS; and
- the Community Name to be used in Trap messages received by the NMS.

To properly configure the SNMP Agent on the CyberSWITCH, perform the following steps:

- enable and configure IP
- enable SNMP
- configure community name information
- configure SNMP trap information (if desired)
- change MIB-2 system group objects (if desired)

For the NMS, follow its specific installation instructions. Note that the NMS you are using must also have the latest enterprise MIB (the `ih_mib.asn` file) compiled on its system.

If you are using Cabletron's SPECTRUM® Element Manager™ as NMS, this enterprise MIB is already built into the NMS software.

If you are using a non-Cabletron product for NMS, you must perform the following:

- copy the MIB file `ih_mib.asn` onto the NMS
- compile the new MIB
- set up NMS to monitor the CyberSWITCH

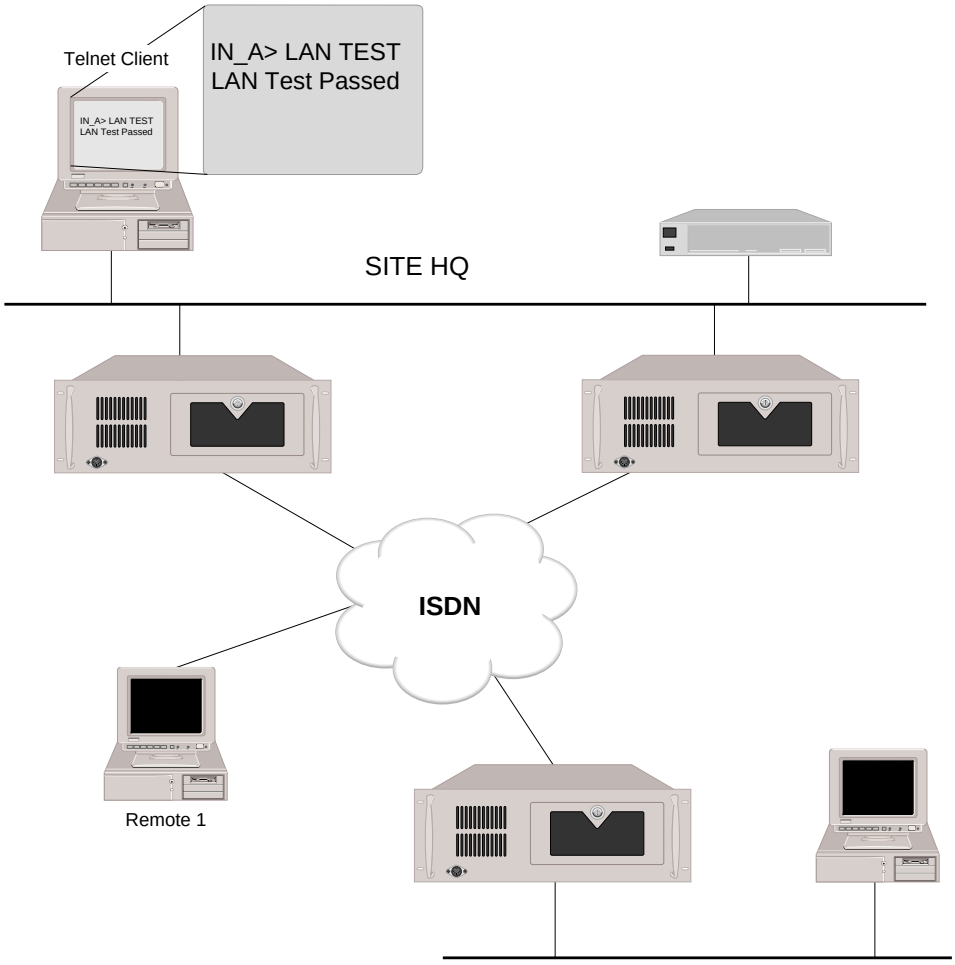
Refer to *Configuring SNMP* for background information on SNMP and details on configuring the SNMP feature.

USAGE INSTRUCTIONS

Normally you will have a GUI NMS (graphical user interface) that will display a picture of the network. You will then select the desired CyberSWITCH and display the desired MIB information. As an example, the information displayed in the *dr* command would be located in the MIB structure under:

[private]
[enterprises]
[networkExpress]
[ih000]
[ih000StatusReports]
[ihStatusReportTable]

TELNET



SITE.2

Telnet is the standard way of providing remote login service. With Telnet, any user on the LAN or WAN executing a standard Telnet client program can remotely login to the CyberSWITCH and get an CyberSWITCH console session. When you have an active console session, CyberSWITCH commands can be entered as if you have a locally-attached keyboard and monitor. Once you use Telnet to login to the CyberSWITCH, it is possible to make configuration changes to the CyberSWITCH using CFGEDIT or the Manage Mode commands.

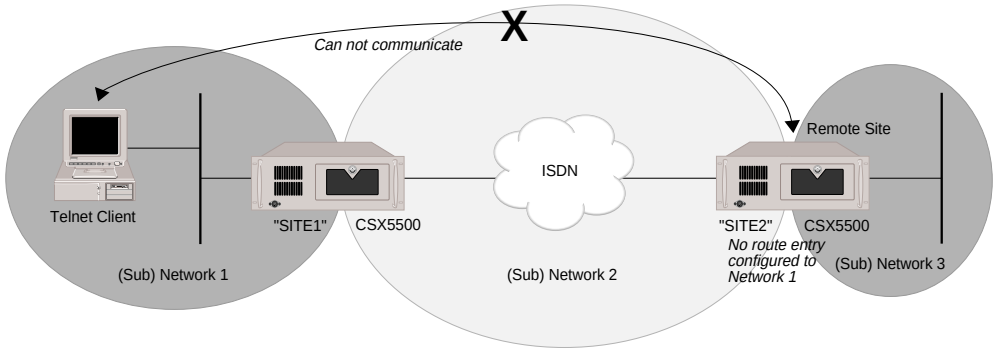
In the first Telnet illustration (see previous page), the Telnet client is not an CyberSWITCH. It is also possible to use the CyberSWITCH as the Telnet client. This allows you to remotely manage an CyberSWITCH with an CyberSWITCH. The benefit from this is you can now use an CyberSWITCH at your site to perform system maintenance, for example configuration changes, on a remote CyberSWITCH.

The two pictures below illustrate the advantage of the CyberSWITCH Telnet client feature. The first example network shown illustrates previous CyberSWITCH releases. In this example, the administrator forgot to configure a static route on the remote site, System 2. Because System 2 is not

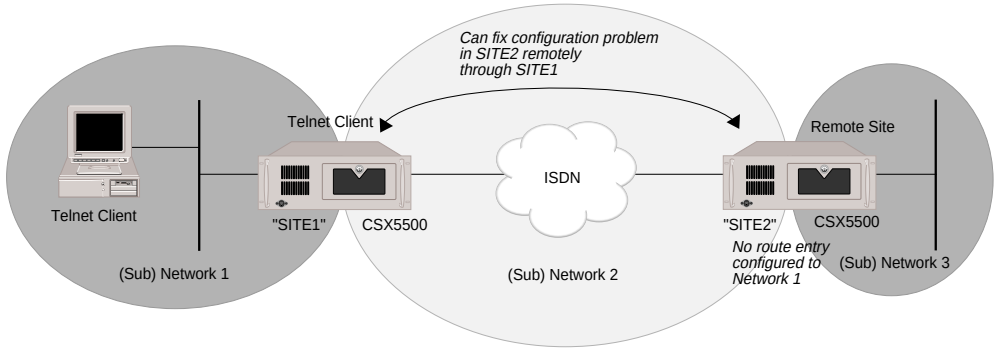
on the same subnetwork as the Telnet client on System 1's LAN, a static route is needed to allow System 2 to communicate with devices on Network 1. Because the CyberSWITCH had no Telnet client capabilities in previous releases, the only way to fix the problem was to physically go to the remote site and add a static route.

The second example network shown illustrates the current CyberSWITCH release. System 1 has Telnet client capabilities, and therefore can simply Telnet to System 2 and add the needed static route.

EARLIER RELEASES:



CURRENT RELEASE:



INSTALLATION AND CONFIGURATION

Telnet is available by default when IP routing is enabled. No installation or configuration steps are required.

USAGE INSTRUCTIONS

To access the CyberSWITCH using Telnet, you must have a Telnet client software package. A Telnet client software package is built into the CyberSWITCH. With the CyberSWITCH acting as the Telnet client, simply enter the `telnet <ip address>` command to Telnet into the target host. Refer to the *System Commands* chapter for a complete listing of available Telnet commands.

If you are using a PC or a workstation as a Telnet client, it must have a Telnet client software package. From the Telnet client package, issue the command that will allow you to connect to the

IP address of the CyberSWITCH. You will then be presented with the "`Enter Login id:`" prompt. Now enter commands as if directly connected to the CyberSWITCH.

When finished with the session, enter the *`exit`* command at the system prompt to end the session with the CyberSWITCH.

Terminate the Telnet session by typing *`logout`*. This will ensure that the Telnet session has been terminated, regardless of the specific Telnet client used.

Notes: If you need to quit then restart the CyberSWITCH for some reason (for example, to have CFGEDIT changes take effect) issue the *`restart`* command. Then reestablish your Telnet session.

If you lose your Telnet connection within 10 seconds of entering the *`restart`* command, the command will not be executed.

WIN95 DIAL-UP NETWORKING

Many dial-up client software packages support a terminal type of connection. One such popular package is Win95 Dial-Up Networking. The CyberSWITCH can handle these terminal-type connections through its digital modem feature, thus providing yet another means of remote management. Refer to *Default Async Protocol* for details on CyberSWITCH configuration requirements.

This section describes how to set up Win95 dial-up networking for a terminal-mode connection to the CyberSWITCH. Specifically, it details:

- the setup of a new number for dial-up networking
- the process of dialing a newly set-up number

SETTING UP A NEW NUMBER

On the remote PC running Windows 95 software:

1. Click *Start*, *Programs*, *Accessories* and then *Dial-Up Networking*. (Or, you may get to the same location by clicking *My Computer*, then double clicking on *Dial-Up Networking*).
2. Double click on *Make New Connection*:
   - Provide name of the computer you are dialing to, and
   - Select modem type
3. Click *Configure*. Three tabs will be displayed:
   - *General* tab:
     - Select com port to which your modem is hooked up.
     - Select modem's maximum speed.
   - *Connection* tab, *Connection Preferences*:
     - Set the following: *Data Bits, 8*; *Parity, none*; *Stop Bits, 1*.
     - *Port Settings* and *Advanced* may remain at default values.
   - *Connection* tab, *Call Preferences* may remain at default values.
   - *Options* tab should remain at default values for PPP connections; for remote management, select *Bring up terminal window after dialing*
4. Click *OK* to accept these values and return you to the modem name / type screen. Click *Next*.
5. Provide *Area code* and *Phone number* of the network you are trying to dial. Also identify the country of the network Click *Next*.
6. Confirm your choices. Click *Finish* to proceed, or *Cancel* to abort the new number shortcut.

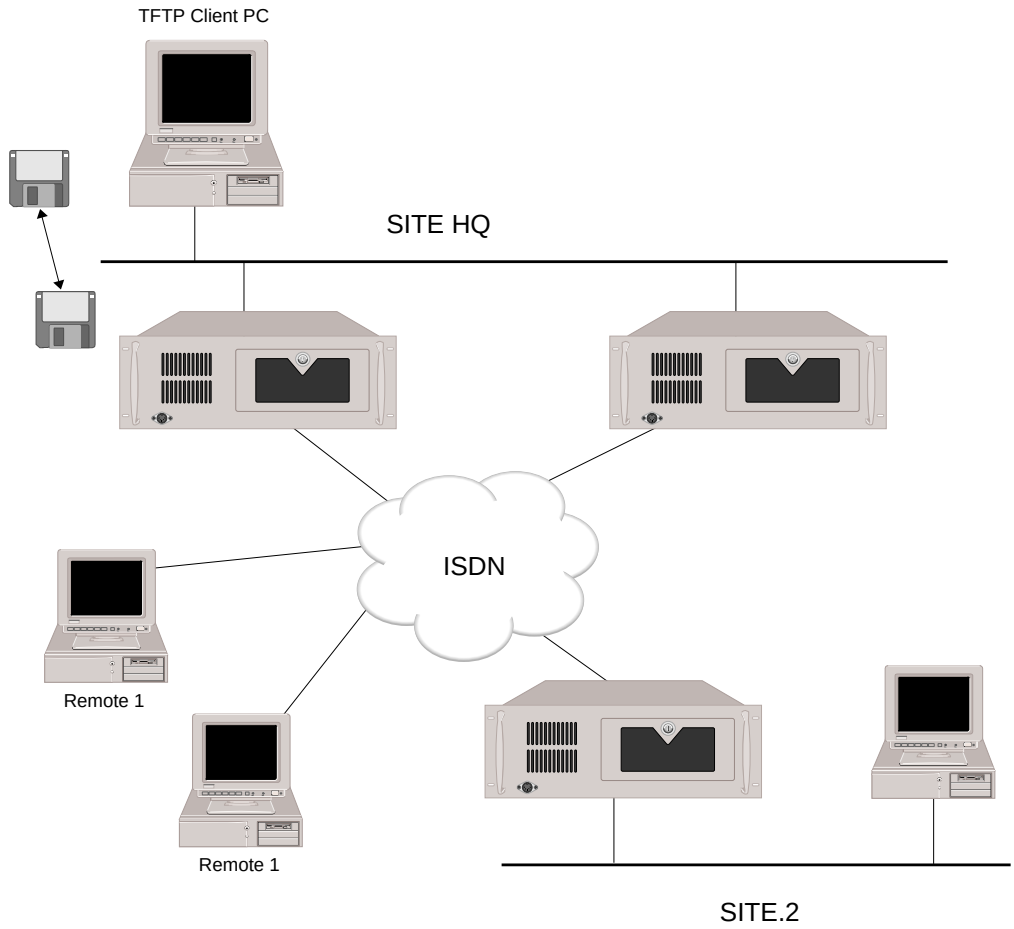
SETTING UP SERVER TYPE

1. After setting up a new number, a new dialing icon will be displayed under *Dial-Up Networking*. (It will have the name you've assigned the new connection). Select this item, click *File*, and then *Properties*.
2. Click *Server Type*. Pick options you want, and identify which protocols your network allows.
3. Click *TCP/IP Settings*. Click *Specify an IP Address* and provide the IP address of your machine. Click *OK* when finished.

DIALING OUT

1. Double click on your new dialing icon to bring up the *Connect To* screen.
2. Enter your user name and password. You may change options by clicking the box labelled *Dialing Properties*, but this isn't necessary.
3. Double click on *Connect*. This should place the call.

TFTP



TFTP (Trivial File Transfer Protocol) is the standard way of providing file transfers between devices. With TFTP any WAN or LAN user executing a standard TFTP client program can transfer files to and from the CyberSWITCH. You can control access to the different file types. Statistics concerning the file accesses are available. This feature can be used to retrieve report and statistics files, and to perform remote node configuration.

INSTALLATION AND CONFIGURATION

TFTP is available to the user by default. No installation or configuration steps are required.

You can limit the access to files by using the ***fileattr*** and ***tftp*** commands of the Dynamic Management feature. The ***fileattr*** command allows you to change the access rights for each file type depending on access level. The tftp command provides the ability to change the TFTP Server file access rights by assigning a user's file accesses rights to the TFTP server. The ***tftp*** command also provides the ability to disable the TFTP client component, TFTP Server component or the whole TFTP feature.

The default file access for the GUEST user is “read” access to all files. The default file access for the ADMIN user is “read” access to the report and statistics files, and “read and write” access to all other files. The default for the TFTP server is ADMIN file access rights. The possible file types and possible accesses for each user are:

Users	*Report Files*	*Statistics Files*	*Config files*	*Other Files*
GUEST	RN	RN	RN	N
ADMIN	RN	RN	RWN	RWN

where:
“R” for *read only* file access
“W” for *write* file access
“N” for *no* access rights for the corresponding file type

Actual files included in the file type categories are as follows:

File category	*File types included in the category*
Report	RPRT_LOG.1 - 10
Statistics	STAT_LOG.1 - 10
Configuration	*.NEI (with the exception of CFGTOKEN.NEI)
Other	All other file types: .EXE, .COM, .TXT, (CFGTOKEN.NEI), etc.

Note: If you use TFTP to copy over configuration files to the CyberSWITCH, the new configuration will not take place until the CyberSWITCH is restarted. This may be accomplished with Telnet session and issuing the `restart` command. The Telnet session must then be reestablished.

USAGE INSTRUCTIONS

The CyberSWITCH has both the client and server TFTP components built into it. When using the CyberSWITCH as the local client, enter the following command(s) to transfer files:

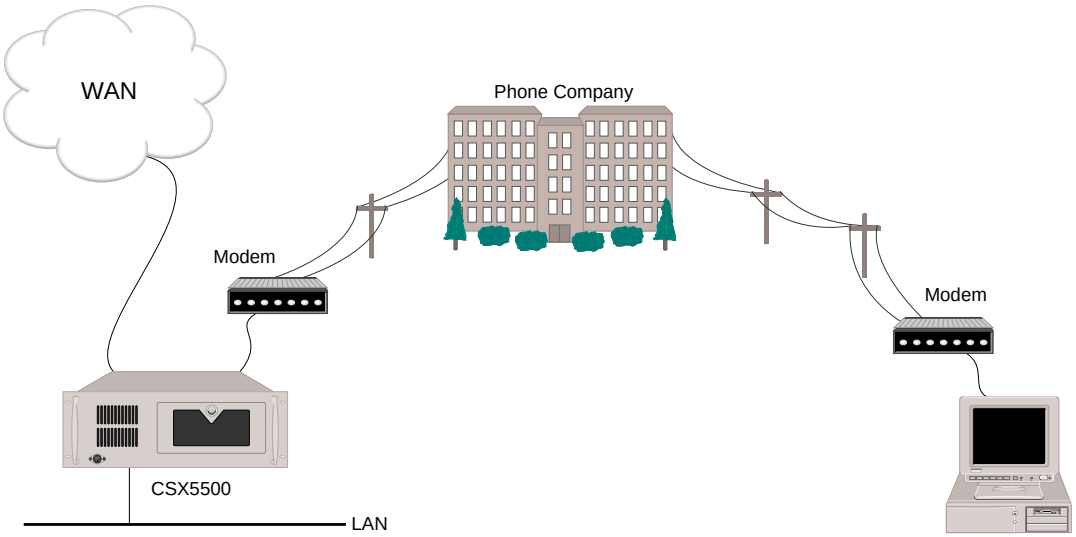
`tftp put` or `tftp get`

The `tftp put` command transfers files to the remote host; the `tftp get` command retrieves files from the remote host. For either command you will then be prompted for the IP address of the remote host, the complete path of local file name, the complete path of the remote file name, and the file mode (binary or ASCII). You will be notified of the status of the transfer.

There is a `tftp stats` command that gives the user statistics on the TFTP feature. Statistics for the server (or remote) side imply that someone from a remote device (either on the LAN or WAN) initiated the request to transferred files to (or from) the CyberSWITCH. Statistics for the client (or local) side imply that the user on the CyberSWITCH initiated the request to transfer files to a remote device. The following statistics are available for both the server and client sides:

- Number of successful file puts
- Number of successful file gets
- Number of failed file puts
- Number of failed file gets
- Total bytes put
- Total bytes get

CARBON COPY



The Carbon Copy feature gives you complete remote management. Any command that you can issue on a local console session can be issued with Carbon Copy. Files can also be transferred between the Manager PC and the CyberSWITCH.

The disadvantage of using Carbon Copy is that a separate telephone line must be connected to each CyberSWITCH being managed. Another disadvantage is that the Manager PC must be an AT compatible PC.

INSTALLATION AND CONFIGURATION

When using the Modem Remote Administration Console, the connection to the CyberSWITCH is done using standard modems. Modems and cables are NOT provided with the CyberSWITCH.

When an CyberSWITCH is delivered, Carbon Copy is configured for a Direct Remote Administration Console. To set your system up for a Modem Remote Administration Console, you must reconfigure Carbon Copy's baud rate and modem type parameters. Instructions for changing these parameters are listed below.

CHANGING CARBON COPY CONFIGURATION PARAMETERS

The Carbon Copy *CCINSTAL* program is available on the CyberSWITCH and on the Manager diskette. (The diskette is available as an option when you order your CyberSWITCH). You can use this program to change Carbon Copy parameters such as password, COM port, baud rate and modem type.

To change Carbon Copy parameters on the CyberSWITCH, terminate the CyberSWITCH by typing *quit*. Next, enter the following command at the MSDOS prompt to change the current directory to "ADMIN":

```
C:\>cd \admin
```

Enter the following command to start up the *CCINSTAL* program:

C:\admin>ccinstal

The Carbon Copy System Parameters screen will appear. Follow the directions on the screen to change parameter settings.

```
A   Comm Port Address  COM1                    Q   Quit, changes not saved
B   Baud Rate          9600                    X   eXit, changes saved
C   Modem Type         Direct Connect
D   Keyboard Handling  USA Keyboard
E   Display Type       Default
F   Menu Colors        White on Blue
G   Working Directory  Default Directory
H   Menu Level Option  Advanced

1   CC Optional Configuration Parameters
2   CCHelp Optional Configuration Parameters
3   Call Table
4   Password Table


    Type letter for selection:
```

After you make all parameter changes, select "X" to save the changes and exit the *CCINSTAL* program. Restart the CyberSWITCH by issuing the command: *start_ne.* After issuing the *start_ne* command, you must again login to the system.

CARBON COPY CONFIGURATION PARAMETERS FOR MODEM USAGE

If you wish to manage your CyberSWITCH via a modem, you will need to make changes to the Carbon Copy configuration parameters. To make these configuration changes, you must have previously installed your internal or external modem. You will also need a locally attached keyboard and monitor.

To change Carbon Copy parameters on the CyberSWITCH, terminate the CyberSWITCH by typing *quit*. Next, enter the following command at the MSDOS prompt to change the current directory to "ADMIN":

C:\>cd \admin

Enter the following command to start up the CCINSTAL program:

C:\admin>*ccinstal*

The Carbon Copy System Parameters screen will appear. Refer to the above section titled *Changing CARBON COPY Configuration Parameters* for a sample screen. Follow the directions on the screen to change parameter settings. The parameters that you may need to change are as follows:

Modem Type
You must change the modem type from the default of "Direct Connect" to your modem's brand name. To make this change, enter a menu selection of "C" (for Modem Type). A list of modem types will be displayed. Arrow down to the type of modem you have installed. If the type of modem you have installed is not included on the list, select Hayes Smartmodem.

You will then be asked if you want to use the Modem's default baud rate. Answer either yes or no by entering Y or N.

Baud Rate
If you wish to enter a new baud rate, enter a menu selection of "B "(for Baud Rate). Continue to press B until the baud rate you desire is displayed.

When you have finished making Carbon Copy configuration parameter changes, enter a menu selection of "X" to save your changes and exit the *CCINSTAL* program. You will be asked if you wish to update the presently running Carbon Copy. Enter "Y" for yes. Carbon Copy will then be reinitialized and you will be returned to the MSDOS prompt.

USAGE INSTRUCTIONS

ESTABLISHING A REMOTE ADMINISTRATION SESSION

When using the remote administration console option, Carbon Copy establishes an administration session with the CyberSWITCH. This section contains a brief description of establishing an administration session using Carbon Copy.

1. If you did not install the Manager software onto the administration console PC (see *Upgrading System Software*) then insert the Manager software diskette into the diskette drive on the administration console PC.

2. Set the administration console PC to the disk drive containing the Manager software (replace "drive letter" with the appropriate administration console PC drive, for example, "A" or "C"). Type:
   `<drive letter>:<return>`

3. Set the administration console PC to the directory containing the Manager software. Type:
   `cd \admin<return>`

4. Load the Carbon Copy CCHELP program on the administration console PC. Type:
   `cchelp<return>`

   Within 3 to 10 seconds, Carbon Copy will be displayed on the screen. The screen is divided into three sections. In the lower right hand corner is the Carbon Copy command screen. It is function-key driven and provides the following commands:

```
[F1]          Call CC Device
[F3]          Capture Screen/Session
[F4]          Review/Replay Captured Image
[F6]          Printer/LOG/DOS Control
[F7]          Terminal Emulation
[F8]          Data Link Maintenance
[F10]         Return to Application
```

5. Choose `Call CC Device` from the Carbon Copy command screen.
   Press: <F1>

   The system will prompt you for a phone number. If you are using remote access with modems, then enter a phone number. If you are directly connected with a null-modem cable, then no phone number is required; just press the enter key.

6. Type: <phone number><return>
   (or just <return> if directly connected)

The system will prompt you for a password. The default password set on each CyberSWITCH is "CC". We recommend that you change this password on each CyberSWITCH using the CCINSTAL program.

7. Type: cc<return>
   (or <your password><return> if the password has been changed)

   If connection with the CyberSWITCH is successful, then the system will remove the Carbon Copy screen. An active administration session now exists with the CyberSWITCH.

   If connection with the CyberSWITCH is not successful, then the system will return an error message in approximately 60 seconds. Check the cable connections, phone number, and password. If the connection with the CyberSWITCH is still unsuccessful, report the problem by using the procedures defined in *Getting Assistance*.

TERMINATING A REMOTE ADMINISTRATION SESSION

This section tells you how to terminate a remote administration session from the administration console PC. You may need this information if you want to make changes to an CyberSWITCH, and then use the same administration console PC to access a different CyberSWITCH.

1. Return to the Carbon Copy command screen.
   Press: <ALT><RIGHT SHIFT> (at the same time)

   This will return the user to the Carbon Copy main screen. In the lower right hand corner, the following commands will be displayed. This command menu is function-key driven.

```
[F1]          Terminate Link
[F3]          Capture Screen/Session
[F4]          Review/Replay Captured Image
[F5]          File Transfer Package
[F6]          Printer/LOG/DOS Control
[F8]          Data Link Maintenance
[F9]          Repaint Screen & Return
[F10]         Return to Application
```

2. Choose "`Terminate Link`" from the Carbon Copy command menu. Press:
   <F1>

3. Carbon Copy will ask if you really want to terminate the link. To answer yes, press:
   <return>

4. Choose "`Return to Application`" from the Carbon Copy command menu. Press:
   Press: <F10>

Performing a File Transfer Using CARBON COPY

After a successful Carbon Copy logon, the lower right hand corner may contain the Carbon Copy menu. If the menu is not present, display it by pressing the <ALT> and <RIGHT SHIFT> keys simultaneously.

```
[F1]          Terminate Link
[F2]          Switch Voice to Data Mode
[F3]          Capture Screen/Session
[F4]          Review/Replay Captured Image
[F5]          File Transfer Program
[F6]          Printer/LOG/DOS Control
[F7]          Terminal Emulation
[F8]          Data Link Maintenance
[F10]         Return to Application
```

To initiate the File Transfer Program, press the function key <F5>.

The file transfer facility will display a one page tutorial. The administration console PC is considered the LOCAL PC. The CyberSWITCH is considered the HOST. To copy files, you issue a command similar to a standard MSDOS copy command and supply the proper prefix to the file paths. For example:

COPY LC:NETWORK.NEI HC:\CONFIG\NETWORK.NEI

where:
L=Local
H=Host

This command will copy the NETWORK.NEI file from the current directory on the administration consoles PC's C: drive to the CyberSWITCH's C:\CONFIG directory. This downloads files from the administration console PC to the CyberSWITCH. To retrieve files such as system logs from the CyberSWITCH, simply reverse the copy procedure.

If you find you need to create subdirectories, rename files, type documents, or other similar file manipulations, you can do so without leaving Carbon Copy. The file transfer facility offers DOS command equivalents to RENAME, TYPE, MKDIR, DIR, and several other popular file manipulation commands. Simply type HELP at the prompt to get more information.

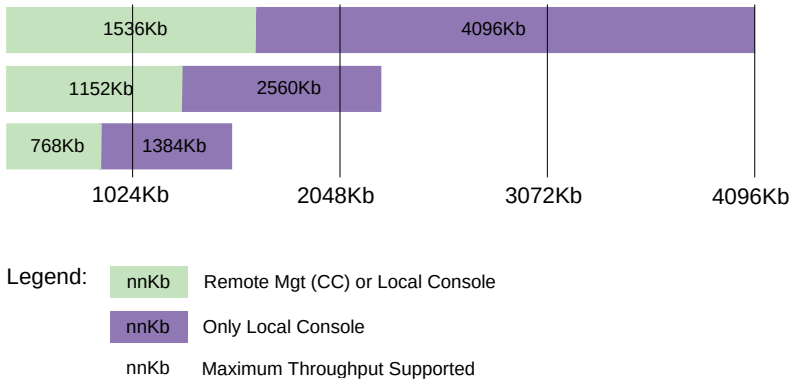
After you finish copying files and want to log-off, select Terminate Link from the command menu. Press: <F1>.

Then select Return to Application from the command menu. Press <F10>. This will return you to the DOS prompt.

RUNNING WITHOUT CARBON COPY

If you plan to use one or more dedicated links of 1Mbps or more, you may wish to increase your system's performance by running without Carbon Copy.

For each Platform, the chart below compares the maximum throughput supported with remote management (running Carbon Copy) compared to the maximum throughput supported with running only a local console (running without Carbon Copy). As shown, the higher the maximum throughput supported, the greater performance improvement there is when Carbon Copy is not running.



Note: The above graph represents the guaranteed throughput without CRC errors. The actual throughput may be higher.

REMOVING CARBON COPY

To remove Carbon Copy from your system:

1. QUIT from the CyberSWITCH.
2. At the DOS prompt, type “dropcc”.
3. Reboot your CyberSWITCH.

NULL MODEM CONNECTION

To use Carbon Copy via a local NULL modem connection to make configuration changes, follow the steps listed below:

1. Insert Disk 1 from your Installation or Upgrade disk set labeled R2.3I13 or later, and reboot.
2. Carbon Copy will now be available via a NULL modem connection to the Serial Port.
3. Once the configuration changes have been made, remove the floppy and reboot your CyberSWITCH. Running the system with Disk 1 inserted is not recommended.

ADDING CARBON COPY

If you wish to restore remote management to your system, re-add Carbon Copy by following the steps below:

1. QUIT the CyberSWITCH.
2. At the DOS prompt, type “addcc”.
3. Reboot your CyberSWITCH.

Note: Carbon Copy is a registered trademark of Microcom Systems, Incorporated.

SYSTEM COMMANDS

OVERVIEW

Two classes of system administration commands are available on the CyberSWITCH: guest commands and administrator commands. Guest commands provide current operational information only, and are available to all security levels. Administrator commands allows access to the complete system command set.

The log-in to the system controls command access. Each access level (guest or administrator) is protected by a unique log-in password. This capability allows managers to assign different responsibility levels to their system administrators.

General operation commands immediately follow this discussion. These commands are divided by functions. Specific feature commands begin on page 591. These commands are arranged alphabetically. For a tabularized listing of system commands, refer to the *Command Table*.

Note: When there are a group of related commands, a help screen is available. For example, to display the help screen for all of the *br* commands, enter *br?* at the system prompt.A screen will then be displayed that includes the available br commands, the syntax for each command, and a definition for each command.

ACCESSING ADMINISTRATION SERVICES

CyberSWITCH software must be running in order to access Administration Services. To start the system, type *start_ne* at the DOS prompt.

The following commands are available for system login:

admin

Logs you into the system and provides access to all system commands. The system will ask you to enter or set the password for administrator level access. Be careful, passwords are uppercase and lowercase sensitive.

admin<00><01><02>...<99>

If you have configured multiple administration login names on your off-node server, you must use one of the configured names to log into the CyberSWITCH. The acceptable names are *admin00* through *admin99*. Proper login provides you with access to all system commands. The system will ask you to enter or set the password for administrator level access. Be careful, passwords are uppercase and lowercase sensitive. (Note: This command is not available for local access.)

guest

Logs you into the system and allows the user access to the commands for viewing operational information only. All other commands for changing information on the system are not available. The System will ask you to enter or set the password for guest level access. Be careful, passwords are uppercase and lowercase sensitive.

exit
Terminates the administration session by logging-out the current administrator. You can start another session by using one of the two log-in commands outlined above.

logout
Terminates the administration session by logging-out the current administrator. You can start another session by using one of the two log-in commands outlined above.

pswd
Changes the password for the current access level (administrator or guest). Your password must be a 3 to 8 nonblank character string. Be careful, passwords are uppercase and lowercase sensitive.

SETTING THE IP ADDRESS

The following administrative command allows you to make changes to the system's default IP address without using the CFGEDIT utility. The system handles this command as if you were in CFGEDIT mode, and saves changes automatically. You must then *restart* your system in order to have these saved changes take effect. To change the system's default IP address, issue the following command:

ipconfig
Allows you to change default IP address information by prompting you for the following:
- IP address
- number of significant bits in subnet mask
- IP address of default gateway (or "0" if none)

After responding to the prompts, the system will ask you if you wish to restart the system in order to put into effect these changes.

ACCESSING DYNAMIC MANAGEMENT

The Dynamic Management feature provides a "real-time" management mechanism that allows changes to system parameters without interrupting the current execution state of the system software. This feature consists of a series of console commands that allow you to display current system parameters, change many parameters dynamically, and write changes to disk files so that they remain permanent.

All dynamic management commands must be issued through a special mode of operation called Manage Mode. To enter Manage Mode, type the following command at the system prompt:

>manage

Once Manage Mode is entered, the prompt changes from *">"* to "MANAGE>".While operating in Manage Mode, Manage Mode commands are the only commands available. All other system commands are ignored until you enter the *exit* command to return to normal system command mode.

VIEWING OPERATIONAL INFORMATION

The following commands are used to view system operational information:

?
Displays a help screen outlining all of the commands that are available.

br stats
Displays the current system packet statistics. Refer to *Bridge Statistics*, for a list of available statistics and their definitions.

cls
Clears the administration screen.

cs
Displays the list of connected devices along with the data rate for each device. The output for this command contains the connection time for each device along with a detailed breakdown (per connection type) of channel usage and available data rates. If there is at least one device connected, the display will look as follows. Note that a "more" mechanism will be used when the number of connected devices exceeds a full screen. If there are no devices connected, the *cs* command does not produce any output.

```
[System Name]> CS

                 Number of Channels        Data Rate (Kbps)      Connect Time
Device Name       Swi Ded FrR X25 Tot   Swi Ded FrR X25   Tot (hr:min:sec)
----------------   ------------------   --------------------   -----------
Tokyo               1   0   0   0   1    64    0   0   0    64    00:31:39
Ann Arbor           1   1   0   0   2    64   64   0   0   128    12:22:18
New York            4   0   0   0   4   256    0   0   0   256    04:02:22
```

da
Displays reports of authentication messages. Refer to the *System Messages* chapter for message definitions.

dr
Displays reports of system messages. Refer to the chapters titled *System Messages* or *Trace Messages* for message definitions.

ds
Displays system statistics. For details on the available system statistics refer to the *System Statistics* chapter.

list [file name]
Displays the indicated file.

For example, to display the Release Notes, enter the following command:
list rel_note.txt

The "more" mechanism is used to view the indicated file. To view the next section of the file, simply press any key (except *<escape>*). The system will automatically return to the normal

system prompt after the entire file has been displayed. If you are viewing the Release Notes, press the *<escape>* key to exit the release notes and continue with the installation.

If the file name is incorrect, the following message will be displayed:

```
Cannot find file "file name"
```

mc

Displays the Connection Monitor screen. This screen provides information on the remote sites to which the system is currently connected. The system updates the display as connections are added or removed.

To display the Connection Monitor screen, Telnet and the terminal emulator must both be set as the same terminal type. Use the *term set* command to do this.

Note: The *mc* command is also available if you are remotely connected to the CyberSWITCH by Telnet.

neif

This command will display the system interface table. This table provides information for each of the system's physical interfaces, including interface name, interface type, slot and port number, and the operational status of each interface (up or down). This information can help to determine system problems by identifying those physical interfaces that are not operating as expected. Refer to the following example:

```
[System Name]> NEIF

id Name              Type              Slot        Port        Status
-- ----              ----              ----        ----        ------
1   Ethernet Port 1   Ethernet          3           1           up
2   Ethernet Port 2   Ethernet          3           2           down
3   BRI.LINE.1        BRI D-Channel     1           1           up
4   BRI.LINE.1        BRI D-Channel     1           2           up
5   V.35.LINE         V.35              2           1           down
```

The definitions of the interface types and the associated status possibilities are as follows:

Ethernet
Each Ethernet port is considered an Ethernet interface. An Ethernet interface is "up" if the Ethernet port is capable of forwarding packets to/from the LAN. An Ethernet interface is "down" if the Ethernet port cannot be used to forward packets to/from the LAN.

Basic Rate (D-Channel)
Each Basic Rate line which contains at least one data link is considered a Basic Rate (D-Channel) interface. A Basic Rate (D-Channel) interface is "up" if at least one data link associated with the interface is "up." A Basic Rate interface is "down" if none of the data links associated with the interface is "up."

Basic Rate (Permanent)
Each Basic Rate line which is used by a dedicated access is considered a Basic Rate (Permanent) interface. A Basic Rate (Permanent) interface is "up" if the serial layer 1 is "up" for the line. The dedicated access does not have to be "up" for the interface to be considered "up". A Basic Rate (Permanent) interface is considered to be down if the serial layer 1 is "down" for the line.

Primary Rate (D-Channel)
Each Primary Rate line which contains at least one data link is considered a Primary Rate (D-Channel) interface. A Primary Rate (D-Channel) interface is "up" if at least one data link associated with the interface is "up." A Primary Rate interface is "down" if none of the data links associated with the interface is "up."

Primary Rate (Robbed Bit)
Each Primary Rate line that uses Robbed Bit Signaling is considered a Primary Rate (Robbed Bit) interface. A Primary Rate (Robbed Bit) interface is "up" if the serial layer 1 is "up" for the line. A Primary Rate (Robbed Bit) interface is considered to be down if the serial layer 1 is "down" for the line.

Primary Rate (Permanent)
Each Primary Rate line which is used by a dedicated access is considered a Primary Rate (Permanent) interface. A Primary Rate (Permanent) interface is "up" if the serial layer 1 is "up" for the line. The dedicated access does not have to be "up" for the interface to be considered "up". A Primary Rate (Permanent) interface is considered to be down if the serial layer 1 is "down" for the line.

V.35
Each V.35 line which is used by a dedicated access is considered a V.35 interface. A V.35 interface is considered "up" if the serial layer 1 is "up" for the line. The dedicated access does not have to be "up" for the interface to be considered "up". A V.35 interface is considered to be "down" if the serial layer 1 is "down" for the line.

RS232
Each RS232 line which is used by a dedicated access is considered an RS232 interface. An RS232 interface is considered "up" if the serial layer 1 is "up" for the line. The dedicated access does not have to be "up" for the interface to be considered "up". An RS232 interface is considered to be "down" if the serial layer 1 is "down" for the line.

sp

This command pertains to semipermanent connections. This command will list each semipermanent device, as well as the connection status, initial data rate and current data rate for each semipermanent device. The connection status will be one of the following:

CONNECTED
The system is connected to the device at the initial data rate or greater.

OVERRIDDEN
The *disc device* command was issued on this device. The system will not attempt to call again until a *call device* command is issued, or the system is rebooted.

NOT CALLABLE
This device cannot be called. Check phone number, device type or existence of the device name in the database.

REJECTED
The remote device answered the system call, but rejected negotiations. The system stops calling attempts until a *call device* command is issued, or the system is rebooted.

TRYING
The system is attempting to call the device. Some connections may be up, but not at the initial data rate.

`status`
Displays initialization, current status, and connection information, as well as any errors that have been detected. For details on these messages, refer to the section titled *LCD Message Groups* found in the *LCD Messages* chapter.

`time`
Displays the current system time. This can be useful when viewing system messages or statistics.

`ver`
Displays the version number of the software that is currently running on the system (II, III, etc.). In addition, it displays all other custom information for this copy of the system software, such as the platform, the installed resources, and the hardware resource revision information. Note that T1_E1_PRI-1 indicates the PRI-23/30 adapter.

The *ver* command also displays a connections table. It displays the connection lines for features that are loaded only. Consider the following example of a connections table:

Capacities	Potential	Actual
Physical Connections	8	8
X.25 Connections	32	32
Frame Relay Connections	48	33
Combined Maximum Connections	88	33

Description:
- The first column is the *connection type*.
- The second column is the *potential number of connections*.
- The third column is the *actual number of connections possible*. The actual number may differ from the potential number due to memory constraints.
- The *combined maximum* line shows the maximum number of connections possible for all types combined. If the potential and actual column do not match on this line, then there are not enough connections for all the connection types to use their respective maximum number of connections at the same time.

For our example, the most connections possible without memory limitations is 88. This is the sum of all the connection types. Since there is not enough memory for 88, the actual number of connections available is less than that amount (33). This means that any of the following combinations of connections would be allowed:

Physical Connections	X.25	Frame Relay
8	25	0
0	32	1
0	0	33
2	2	29

If there was enough memory for all connections, the connection table would reflect both potential and actual connections as the same number.

wan stats
Displays the current system WAN connection statistics. Refer to *WAN Statistics*, for a list of available statistics and their definitions.

From the "Connection Monitor" screen you can press:

<Arrow Keys>
To select a site that is currently connected.

<Enter>
To view throughput monitoring for the selected site. Refer to the section titled *Viewing Throughput Information,* for details.

<Esc>
To exit the Connection Monitor screen.

VIEWING THROUGHPUT INFORMATION

The Throughput Monitor screen displays the system throughput monitoring feature in action. To enter this screen:

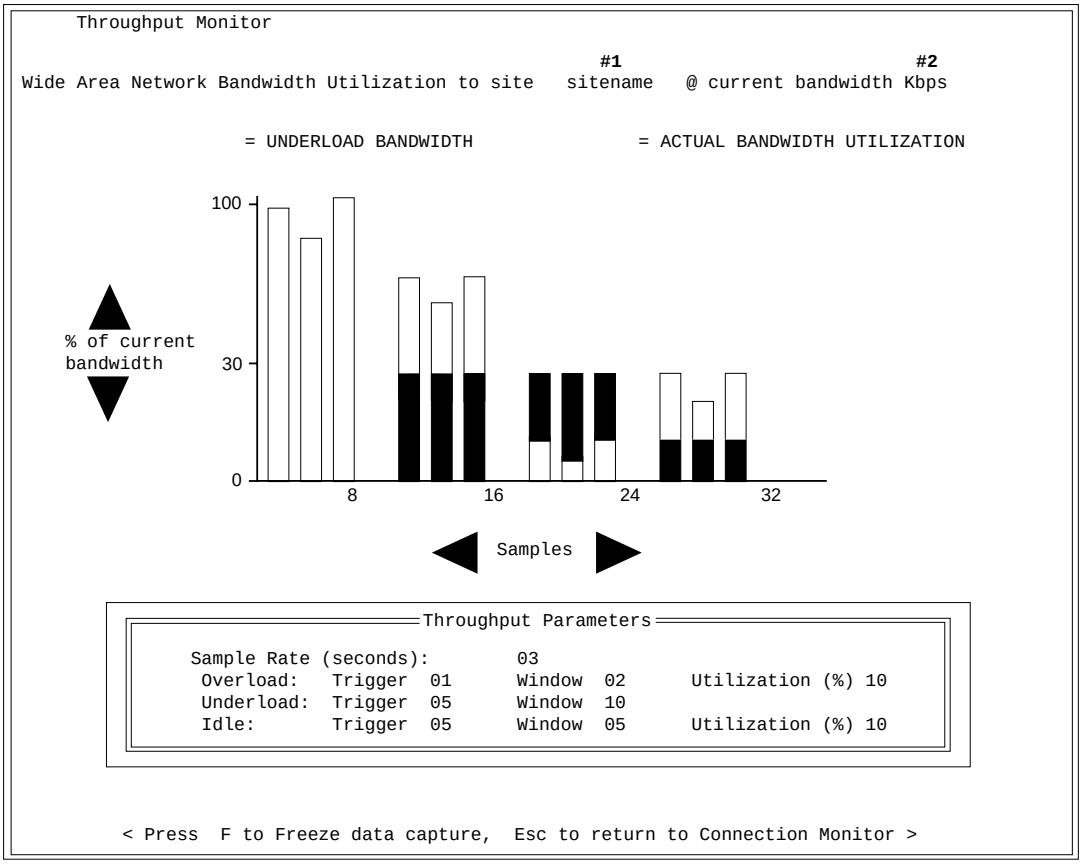
1. Issue the *mc* command to display the connection monitor screen.

2. Use the <arrow keys> to move the cursor down to the specific site for which you would like to view throughput information.

3. Press <enter> to display the throughput monitor screen for that site.

Throughput monitoring information can be very useful for fine-tuning your bandwidth configuration parameters. Note that this feature is not available through a Telnet session. Refer to the *Configuring Call Control* chapter for a complete description of throughput parameters.

The actual bandwidth utilization, along with the current underload setting, is displayed for each throughput sample. After 32 samples are displayed, the newest sample is displayed at position 32 and all other samples are shifted left one position.



Note: If data compression is being used, an extra line will be displayed on the Connection Monitor screen that will provide the compression and decompression ratios, and the estimated throughput. The estimated throughput is calculated as follows:

est. thruput (in Kbits/second) = [(uncmp bits + undmp bits)/sample period)]/1000

Where uncmp bits = the number of uncompressed bits
undmp bits = the number of undecompressed bits
sample period = configured length of the sample period

THROUGHPUT MONITOR CONTENTS

#1. Indicates the site name for the connected site that was selected on the Connection Monitor screen.

#2. Indicates the current bandwidth in place to the connected site. This number will be updated as calls are added or released.

#3. Example of three samples where actual bandwidth utilization was around 95% and underload was not being monitored (probably because only one connection was in place). In this example, overload is occurring on all three samples.

#4. Example of three samples where actual bandwidth utilization was around 70% and underload was being monitored at around 25% utilization of current bandwidth. In this example, overload is occurring on all three samples.

#5. Example of three samples where actual bandwidth utilization was around 10% and underload was being monitored at around 25% utilization of current bandwidth. In this example, underload is occurring on all three samples.

#6. Example of three samples where actual bandwidth utilization was around 25% and underload was being monitored at around 10% utilization of current bandwidth. In this example, neither overload nor underload is occurring.

From the Throughput Monitor screen, press:

f To freeze the current throughput monitor display.

r To resume the display of throughput monitor samples.

<esc> To exit the Throughput Monitor and return to the Connection Monitor screen.

SAVING OPERATIONAL INFORMATION

The following commands are used to save system operational information to disk:

wr
Writes the current system messages to disk file.

ws
Writes the current system statistics to disk file.

Note: For details on these disk files, refer to the chapter titled *Software Overview*.

CLEARING OPERATIONAL INFORMATION

The following commands are used to clear current system operational information:

er
Erases the current system messages held in memory.

es
Erases the current system statistics held in memory.

CONFIGURATION-RELATED COMMANDS

The following commands provide configuration file information, and restore backup configuration files:

cfg

Provides information on the status of system configuration changes. With Manage Mode and / or CFGEDIT, you can make changes to the system configuration. (This, in turn, changes the .nei files.) If you do not commit these changes (Manage Mode) or restart your system (CFGEDIT), these changes do not become current. This command identifies whether or not changes have been made which are not yet current. The command will display the following information:

```
Unsaved Manage Mode Changes Exist.........YES (or NO)
               Cfgedit Changes Have Been Saved...........YES (or NO)
               System Data Differs from Config Files.....YES (or NO)
               To Synchronize System Data With Config Files........
                                 RESTART THE SYSTEM
                                   (or COMMIT FROM MANAGE MODE)
```

restore

Replaces the current configuration files with the configuration backup files (.bak files) located in the \CONFIG directory, thus restoring the previous system configuration. Because this command will destroy your current configuration, a warning is displayed when issued:

```
WARNING:This command overwrites your current configuration files. Are you sure
you want to restore your old configuration? (Y or N)
```

If you indeed want to restore the old configuration, type "Y". If not, type "N" (default).

Note that you must have saved configuration changes at least one time before the *restore* command will work.

TERMINATING AND RESTARTING THE CYBERSWITCH

The following commands are used to terminate and restart the system program:

quit

Terminates the system program. You may need to "*quit*" in order to perform a system function such as a system upgrade, configuration change or a configuration backup.

start_ne

Restarts the system program and is available only after you issue the *quit* command. After issuing the *start_ne* command, you must again login to the system.

restart

Generally used from a remote site (when using Telnet or TFTP), although it is functional from a local console as well. The *restart* command reboots the system and automatically starts up the system software. Issue this command after making configuration changes with CFGEDIT, in order for these changes to take effect.

If you prefer, you can make configuration changes and store them remotely. Later, you can transfer the changes (the .nei files) to the system using TFTP. In order for these changes to take

effect, you would need to issue the *restart* command from the Telnet session of your remote terminal.

Note: If you lose your Telnet connection within 10 seconds of entering the *restart* command, the command will not be executed.

SETTING THE DATE AND TIME

The following commands are used to set the date and the time on the system:

date <month, day, year>

Changes the date on the system as specified. The <month> can be specified as a numeral from 1 to 12, spelled out in full (January), or abbreviated to 3 letters (JAN). The <day> can be any legal date within the month specified. (For example, 1 through 31 would be legal dates for January.) The year may be specified in its entirety (1995) or by its last two digits (95). Commas, dashes, and white space are all acceptable separators.

time hours:minutes <:seconds> <AM/PM>

Changes the time on the system as specified. The hours can be from 0 - 23 in military time, or from 1 - 12 in civilian time, with an optional AM / PM indicator. The "seconds" parameter is also optional. If "P" is included (indicating "PM"), 12 is added to the hour. White space is unimportant.

If the time command is issued without any parameters, the system will report the current time. Parameters following the time command are interpreted as an attempt to make a change.

TERMINATING ADMINISTRATION SESSIONS

The following commands are used to display and to terminate active administration sessions.

session

This command will display the current active administration sessions. The example screen below illustrates the format in which this information is displayed:

```
Login-Id Sess-Id   Date/Time Idle(sec) Command   Type (from)
-------- -------   --------- ---------- -------   -------------------
ADMIN       0    Aug 15 13:50     51     MANAGE    Console
ADMIN     257    Aug 15 13:55      0     SESSION   Telnet (199.120.211.120)
```

The fields in this display are defined as follows:

Login-Id

The access level associated with the session. Possible access levels include:

admin: administrator access
guest: guest access
nobody: someone has initiated a Telnet session with the CyberSWITCH but did not login.

Note: If you have configured multiple admin login names on your off-node server, the *login-id* field will not distinguish between the various names. Use the *sess-id* field to help identify the different admin users.

Sess-Id
The session Id number associated with the session.

Date/Time
The date and time the session was initiated

Idle (sec)
The number of seconds the connection has been idle.

Command
How the administration session was initiated. Initiation methods include:
manage - the user is in the Manage Mode
session - the user is using a Telnet session

Type (from)
The type of session. Possible session types include:
console - a session through the local console
telnet - a Telnet session

Note: If you have configured multiple admin login names on your off-node server, the *login-id* field will not distinguish between the various names. Use the *sess-id* field to help identify the different admin users.

`session kill <session id>`
Terminates the session specified by the session Id. Useful for terminating sessions that have been idle for an extended period of time.

APPLETALK ROUTING COMMANDS

The following commands are used to display AppleTalk information and statistics.

`atalk arp`
This command will display the AARP (AppleTalk Address Resolution Protocol) cache. AARP is used to map between a device's AppleTalk address and their physical address. A sample output screen is shown below:

```
Entry 1: Address 21.1 @ 08:00:07:8f:90:04, valid
```

where:
Address 21.1 is Entry 1's AppleTalk address.
08:00:07:8f:90:04 is Entry 1's physical address (MAC address).
valid is the state of Entry 1's address. The state value can be either valid or pending. If the state is valid, an address will have been logged (as shown). If the state is pending, the address would not yet be logged, and would appear as 00:00:00:00:00:00.

`atalk ping <dnet>.<dnode> [timeout/dnnn]`
This command will allow you to "ping" a specified device. If the ping is successful, you have connectivity to the device. If it is unsuccessful, you do not have connectivity to the device.

The parameters for this command are:

dnet
Required parameter. The destination network number.

dnode
Required parameter. The destination node Id.

timeout
Optional parameter. The number of seconds to wait for a reply message. The valid range is from 1 to 60 seconds. The default value is 10 seconds.

nnnn
Optional parameter. The data size to be included in the ping packet. The valid range for the data size is 5 to 586 octets. The default value is 100 octets.

An example atalk ping command could read as follows:

```
atalk ping 1.3 30 /d200
```

which would send a ping to node number 3 or network number 1, with a timeout value of 30 seconds, and the data size would be 200 octets.

atalk port

This command will display AppleTalk port information. A sample output screen is shown below:

```
Port 1
     type: LAN          state: UP
     address: 20.20     network range 20-21
     flags: extended   phase-2   soft-seed
     default zone: zone1
     lan port: 1    physical address: 00409A001AB3

Port 2
     type: WAN          state: UP
     address: 30.30     network range 30-31
     flags: extended   phase-2   soft-seed
     default zone: zone1

Port 3
     type: WAN UNNUMBERED state: UP
     address: 20.20 (borrowed)
     remote device: MAC4
```

The fields in this display are defined as follows:

type
The port type. Possible types are LAN, WAN, WAN UnNumbered.

Note that the WAN UnNumbered port information is *not* taken from the previously configured AppleTalk Routing *port information*, but is derived from the AppleTalk Routing *static route configuration* information.

state
The state of the port as it is in the process of coming up. Possible states include:

listen - The port is listening to see if any other routers are out on the network.
probing - The port is probing the network to see if its suggested AppleTalk address is unique, or if it is already in use.

get_info - The port is verifying network information and obtaining the default zone.
get_zones - The port s obtaining a complete zone list for the network.
get_routes - The port is requesting routes from another router on the network (if another router is present).
up - The port is ready for use.
down - The port is not ready for use.
unnum_wait_addr - This state will exist with the following scenario:
When an UnNumbered WAN port sends a locally generated packet that requires a reply, a return address is needed. But, because the port is UnNumbered, it has no address assigned to it that it can use as a return address. To remedy this, the UnNumbered WAN port will "borrow" an AppleTalk address from a local numbered port, knowing that when the reply comes, it will first come to the UnNumbered WAN port. If the UnNumbered WAN port attempts to "borrow" an address, but there are no numbered ports up, the *unnum_wait_addr* state exists; the WAN UnNumbered port is waiting for an address.

address
The port's AppleTalk address.

network range
For a LAN port, this specifies the AppleTalk network range of the LAN segment to which the port is connected. For a WAN port, this specifies the AppleTalk network range of the logical segment to which the port is connected. For NonExtended networks, the range will appear as one number (for example, 121-121). For UnNumbered ports, the range will appear as either 0-0 (nonextended networks) or 0.0-0.0 (Extended networks). Note that if the network is nonextended (phase 1), this field will be *network* (and will display a singular value) as opposed to *network range* (which displays a range).

flags
This will reflect any flags that have been activated for the indicated port. Possible flags are:
extended - This flag is triggered if a network range has been configured for the port.
phase-1 - This flag is triggered if the NonExtended network type is configured for the port.
phase-2 - This flag is triggered if the *phase-1* flag has *not* been triggered.
probe-invalid - This flag is triggered if the port sends out a probe to see if its suggested AppleTalk address is unique on the network, and a response comes back indicating that the address is already in use, and cannot be used by this port.
soft-seed - This flag is triggered if the port is *not* configured in the discovery mode (it is configured with a suggested network range). Its classification as a *soft*-seed router indicates that it does have a suggested network range, but that range can be overridden if necessary.

default zone
The port's configured default zone.

LAN port
For LAN ports only. Indicates the Ethernet resource's port number associated with this AppleTalk LAN port.

physical address
For LAN ports only. The device's MAC address.

remote device
For WAN UnNumbered ports only. The remote device configured to use this port.

`atalk port stats [clear]`

This command will display or clear current AppleTalk port statistics. Refer to *AppleTalk Port Statistics*, for a list of available atalk port statistics and their definitions.

`atalk route`

This command will display AppleTalk static route information. A sample output screen is shown below:

```
network range     distance       state      next hop    zones valid
-------------     --------       ------     --------    -----------
 225 - 226          0            good         0.0          TRUE
```

The fields in this display are defined as follows:

network range
The remote AppleTalk network range reachable through this static route. Note that if there is only a single network number instead of a range, that number will appear twice under the network range field.

distance
The number of AppleTalk routers that are traversed in order to reach the destination AppleTalk network.

state
The state of the route. Possible values are:
good - This indicates that this is a valid route.
bad - This indicates that the indicated router has not been heard from in a while; it has timed out. Therefore, it is no longer a valid route.

next hop
The AppleTalk address of the next hop device that provides access to the destination AppleTalk network. If the distance = 0, and the next hop = 0.0, this indicates that there is no router between the port and the destination. If the distance ≠ 0, and the next hop = 0.0, this indicates that the static route is over an UnNumbered port.

zones valid
For every route there is a set of associated zones. When a device has learned the complete list of zones for that route, the zones valid field will display TRUE.

`atalk stats`

AppleTalk statistics are comprised of six subgroups of statistics. The `atalk stats` command displays all six groups of the current system AppleTalk statistics. Refer to *AppleTalk Routing Statistics*, for a list of available AppleTalk statistics and their definitions.

Enter one of the following commands to display a subgroup of the AppleTalk statistics:

`atalk stats ddp`
Displays the AppleTalk Data Delivery Protocol (DDP) statistics.

`atalk stats echo`
Displays the AppleTalk Echo Protocol (AEP) statistics.

atalk stats rtmp
Displays the AppleTalk Routing Table Maintenance Protocol (RTMP) statistics.

atalk stats zip
Displays the AppleTalk Zone Information Protocol (ZIP) statistics.

atalk stats nbp
Displays the AppleTalk Name Binding Protocol (NBP) statistics.

atalk stats atp
Displays the AppleTalk Transaction Protocol (ATP) statistics.

atalk zone
This command will display AppleTalk zone information. A sample output screen is shown below:

```
zone                            network range
-----------------               -------------
zone1                              225 - 226
zone2                              236 - 237
```

The fields in this display are defined as follows:

zone
The AppleTalk zone name for the network that the AppleTalk port is connected to.

network range
Specifies the network range associated with the indicated zone.

BRIDGE COMMANDS

The following commands are used to display bridging information and statistics.

pkt mac
Enables the MAC address monitor display. The MAC Address Monitor screen displays information contained in the LAN frames that are sent over the ISDN connections. The packets represented by the displayed MAC address pairs will not be captured unless the br pkt capture feature is on (enabled).

When the MAC Address monitor is enabled, the CyberSWITCH inspects each LAN frame sent or received over the ISDN connections. It displays the Destination MAC Address, Source MAC Address, and Ethernet type field for each LAN frame.

```
                                MAC Address Monitor

    DEST           SOURCE         TYPE   COUNT       DEST           SOURCE         TYPE   COUNT

90409A000000    00409A001023-L    3C09   00010    00409A001023    00409A001324-R    3C09   00140
00409A001324    00409A001023-L    3C02   00141    90409A000000    00409A001000-L    3C09   00010
90409A000000    00409A002345-L    8137   00015    00409A002345    00409A003217-R    8137   00045
00409A003217    00409A002345-L    8137   00045

                              Number of Packets Received 00406
```

In the above example, the DEST field is the destination MAC address field of the LAN frame. The SOURCE field is the source MAC address of the LAN frame. Next to the source MAC address field is the location of that source address. An "L" next to the source address indicates that this address is "Local" to the CyberSWITCH. That is, it is attached to the Ethernet segment locally connected to the CyberSWITCH. An "R" next to the source address indicates that this address is "Remote" to the CyberSWITCH. That is, it is attached to an Ethernet segment that is connected to a remote ISDN device.

The TYPE field is Ethernet type field of the LAN frame. This hexadecimal field represents the protocol identifier for an Ethernet formatted frame. For an 802.3 formatted frame, it is the length of the data unit.

The COUNT field is the number of frames transferred for that destination address, source address, and Ethernet type combination. The total number of frames is displayed at the bottom of the screen.

To exit the MAC Address Monitor screen and disable the feature, press <Esc> on the Administration console keyboard.

br stats

Displays the current system packet statistics. Refer to *Bridge Statistics*, for a list of available bridge statistics and their definitions.

br stats clear

Clears the current system packet statistics.

CALL CONTROL COMMANDS

The following commands are used to initiate and disconnect calls to devices.

call device <device name>

Initiates a call to the specified device. The entire device name does not need to be entered; only enough letters of the name to distinguish it from any other configured device name. For example, you could enter ***call device sm*** if there are no other devices whose names begin with ***sm***. The call device command can be used to test the Dial Out capability to a specific device. This command is available only when the Authentication mode is "On-node Device Table." To obtain the device name, enter the Manage Mode and issue the ***device*** command. Note that the device name is case sensitive.

To use this command for troubleshooting, you must use the System Call Trace feature to capture any connect and disconnect messages that are generated by issuing the *call device* command. To do this:

1. Erase the current report log by entering *er* at the system prompt.

2. Enable the Call Trace feature by entering *trace on* at the system prompt.

3. Issue the *call device <device name>* command.

4. Display the system log messages by entering the *dr* command at the system prompt.

5. Check the log report for connect messages relating to the remote device you are testing.

In response to the *call device <device name>* command, one of the following responses will be displayed:

`Calling device <device name>`
Indicates that a call request process has been initiated.

`<device name> could not be found in the Device Table`
Indicates that the device name could not be found in the table of configured device names.

`<device name> is already connected`
Indicates that a connection to a device can not be initiated if there is already a connection to that device. The call device command cannot be used to increase bandwidth for an existing connection.

`Call attempt failed`
Indicates that the request could not be executed.

`More than one match for <device name> found in the Device Table`
Displayed if you enter just part of a device name and that part could specify more than one device name. You will be prompted to enter the device name again, in a more specific manner. For example, if *call device Sch* is entered, and there is a device configured with the name Schultz, and a device configured with the name Schmidt, this message would be displayed. You would then need to enter at least *call device Schu* to successfully initiate a call to the device Schultz.

`<device name> is not callable`
Each PPP device in the device database can have one or two phone numbers at which they can be called. This message is displayed if the device has no phone number specified.

`Re-enter the name, or <RET> to cancel`
The device name must be re-entered.

`Unable to prompt for device name at this time`
Indicates that the *`call`* command would prompt you for a device name, but the necessary resources are not available. The recommended actions are as follows:

1. If possible, enter the device name on the command line.

2. If the device name cannot be entered from the command line (for example, the device name contains command line delimiters of a space, a comma, a colon, or a tab), the user can wait for a few minutes and see if any resources become available.

3. If actions 1 and 2 are ineffective, this may indicate an internal problem in the System, please inform your service representative of the occurrence.

`call peer <phone number> [data rate] [device] [bearer]`
Initiates a call to a peer at the given number. Entering the data rate, device, and bearer is optional. We describe each of the optional fields below.

`data rate`
The default data rate value for HDLC calls is *56Kbps*. The default data rate for digital modem calls is *Auto*.

`device`
The valid values are:
- `HDLC`: used for normal HDLC-ISDN calls
- `DM`: used for Digital Modem calls.

`bearer`
This field applies only to Digital Modem calls. The valid values are:
- `SPEECH` (the default if no bearer type is specified)
- 3.1KHZ

The *`call peer`* command allows you to make a connection with another device. For example, to call a site with the configured phone number of 13135552222 and a data rate of 64Kbps, you would enter *`call peer 13135552222 64.`*

To use this command for troubleshooting, you must enable the Call Trace feature to capture any connect and disconnect messages that are generated by issuing the *`call peer`* command. To do this:

1. Erase the current report log by entering *`er`* at the system prompt.

2. Enable the Call Trace feature by entering *`trace on`* at the system prompt.

3. Issue the *`call peer <phone number> [data rate]`* command.

4. Display the system log messages by entering the *`dr`* command at the system prompt.

5. Check the log report for connect messages relating to the remote device you are testing.

In response to the *`call peer`* command, you will see the following message echoed back for informational purposes:

Calling <phone number> at <data rate>, device PPP

The phone number will show what is sent to the switch. Any imbedded dashes will have been removed. The data rate that is used is displayed. If an invalid data rate is entered, the default of 56 Kbps will use used. Because dial out is only provided for PPP devices, the device type is always PPP.

One of the following messages will then be displayed:

`Call initiated`
This response indicates that a *call peer* request was performed. This does not always imply that a request reached the telephone switch.

`Call attempt failed`
This response indicates that the request could not be executed.

Note: The *call peer <phone number>* command will not work under the following conditions:

If PAP or CHAP is enabled and Outbound Authentication is disable, or, if the only security enabled is CLID. In either case, the CyberSWITCH will not be able to authenticate the remote peer. A message will appear in the log to indicate this. Use the *call device <device name>* command instead.

disc device <device name>

Disconnects all calls to the specified device. To obtain the device name, enter the Manage Mode and issue the *device* command. Note that the device name is case sensitive.

In response to the *disc device* command, one of the following responses will be displayed:

`Disconnecting <device name>`
Indicates that the disconnect process has been initiated for the indicated device.

`No active connection to <device name>`
Indicates that the device that you are attempting to disconnect has no active connection. The *mc* or the *cs* command can be used to view the active connections.

`<device name> could not be found in the Device Table`
Indicates that the device name could not be found in the table of configured device names.

More than one match for <device name> found in the Device Table
Displayed if you enter just part of a device name and that part could specify more than one device name. You will be prompted to enter the device name again, in a more specific manner. For example, if *call device Sch* is entered, and there is a device configured with the name Schultz, and a device configured with the name Schmidt, this message would be displayed. You would then need to enter at least *call device Schu* to successfully initiate a call to the device Schultz.

`Re-enter the name, or <RET> to cancel`
The device name must be re-entered.

`Unable to prompt for device name at this time`
Indicates that the *`call`* command would prompt you for a device name, but the necessary resources are not available. The recommended actions are as follows:

1. If possible, enter the device name on the command line.

2. If the device name cannot be entered from the command line (for example, the device name contains command line delimiters of a space, a comma, a colon, or a tab), the device can wait for a few minutes and see if any resources become available.

3. If actions 1 and 2 are ineffective, this may indicate an internal problem in the System, please inform your service representative of the occurrence.

CALL DETAIL RECORDING COMMANDS

The following commands are used to monitor and verify the call detail recording (CDR) feature.

`cdr stats`
Display the CDR statistics. Refer to *Call Detail Recording Statistics*, for the available statistics and corresponding definitions.

`cdr stats clear`
Clears the CDR statistics; setting them all to zero.

`cdr verify`
Generates a "verify" report to all servers that have been configured for CDR use, then typically displays a list of all servers to which it sent the messages. If no log servers or events are configured for CDR, it will report that no messages were sent.

Refer to *Log Commands* for the commands that will allow you to display or erase CDR log reports.

CALL RESTRICTION COMMANDS

When the Call Restriction feature is enabled on the CyberSWITCH, the following command is available through the administration console:

`cr stats`
Displays the current Call Restriction statistics. Refer to *Call Restriction Statistics*, for a list of available statistics and their definitions.

Other Call Restriction commands are available through Dynamic Management. Refer to *Configuring Call Control* for these commands.

COMPRESSION INFORMATION COMMANDS

Compression statistics are only available for connections that are using a compression protocol. The following commands are used to display current compression information:

cmp stats
Displays the compression statistics for all active connections. Refer to *Compression Statistics*, for a list of available compression statistics and their definitions.

cmp stats <device name>
Displays the compression statistics for the indicated device. Refer to *Compression Statistics*, for a list of available statistics and their definitions. Note that the device name is case sensitive.

cmp clear <device name>
Clears the compression statistics for the indicated device. If the device name is omitted, no compression statistics will be cleared. Note that the device name is case sensitive.

cmp clearall
Clears the compression statistics for all devices.

CSM COMMANDS

The primary service is selected through the Connection Services Manager (CSM) GUI. When configuring services, you first add an entry for each service, then optionally configure managing information to designate primary and secondary services for the network's Access Servers. In the past, a service would attempt to TCP connect to all Access Servers configured in its database. The Access Server would consider the first service to TCP connect as its primary server. If that server became no longer available, the next server to connect would take over, and so on. By configuring managing information, you are able to designate a specific primary and secondary server. Refer to CSM documentation for more information about using primary and secondary servers.

primcsm
Displays a message indicating whether or not a CSM is currently acting as a Primary Service. One of two messages will be displayed:

The CSM currently being used as Primary is at: <IP address>.

or

There is currently no CSM connection established.

DHCP COMMANDS

These commands allow you to display or erase DHCP statistics.

DHCP stats
Displays the DHCP statistics. For a listing of available statistics and their definitions, refer to *DHCP Statistics*.

DHCP stats clear
Clears the DHCP statistics.

ip addrpool
Displays the current IP address pool. Refer to the *ip addrpool* command description under *IP Routing Commands*.

DIGITAL MODEM COMMANDS

These commands allow you to display active connections, display or erase digital modem statistics, add or delete individual modems and upgrade modem firmware when necessary.

modem add <slot #> <modem #>
Adds a previously-deleted modem back to the available list for devices (i.e., after testing).

modem delete <slot #> <modem #>
Deletes a modem from the available list for devices. This command is useful in the event you have a faulty modem and wish to temporarily disable it for troubleshooting purposes. Use this command in conjunction with the *modem add* and *modem status* commands.

modem reset <slot #> <modem #>
Resets the specified DM-24 or DM-30 modems on a particular slot. Does not affect other modems on the board. A modem currently in use cannot be reset. DM-8 modems cannot be reset.

modem restart <slot #>
Restarts the digital modem board (i.e., if an unrecoverable problem occurs). This command does not affect any other boards within the system.

modem stats <slot #><modem #>
Displays the digital modem statistics associated with the specified modem. For a listing of available statistics and their definitions, refer to *Digital Modem Statistics*.

modem stats clear <slot #><modem #>
Clears the digital modem statistics associated with the specified modem.

modem status <slot #>
Displays the slots that have valid digital modem (DM) boards. If the command is executed using a specific valid DM board slot, displays the modems available for usage from specified slot.

modem upgrade <slot #> <all>
Installs new modem firmware by reprogramming the specified modem's flash memory.

Periodically, you may want (or need) to add new firmware to DM-24, DM-24+, or DM-30+ modems. To do so, you would need to load the new modem file onto the CyberSWITCH `C:\system` directory. Then to reprogram the modems, issue the *modem upgrade* command, which upgrades all the modems on the card:

modem upgrade <slot #> <all>

Slot number refers to the slot in which the digital modem card resides, and all refers to all modems on the card. Example: *modem upgrade 2 all* upgrades all modems on the DM card in slot 2.

We recommend you monitor the upgrade process by using the `dr` console command. The upgrade process should take approximately one minute. Only after the upgrade process completes for all modems, reset the system.

Note: DO NOT DISRUPT POWER *during* the execution of the modem upgrade process! If power is disrupted, it could result in damage to the modem.

`modem devices`
Displays active digital modem connections by device name. Lists slot number, modem number, and in the case of the DM-24 or DM-30, lists connect parameters.

FRAME RELAY COMMANDS

The following commands are used to display information concerning both the status and traffic statistics of a particular frame relay connection.

`fr a <access n>`
Sets an internal variable. The frame relay `<access n>` will be the assumed current access for all subsequent frame relay system console commands entered. <*Access n*> will remain the current access, until it is changed through issuing another `fr a <access n>` command. The <*access n*> is the access index that is assigned to each frame relay access during the frame relay access configuration.

Note that this command may be used in conjunction with all other `fr` commands. For example, `fr a 1 lmi` would be a valid command, changing the frame relay access to 1 before displaying information relating to the LMI link.

`fr d <DLCI m>`
Sets an internal variable. `<DLCI m>` will be the default DLCI under the currently-selected access, and therefore the assumed context for all subsequent frame relay system console commands entered. <*DLCI m*> will remain the default DLCI until the default is changed through reissuing the `fr d <DLCI m>` command. The DLCI value is provided by the service provider at line subscription time.

For the following frame relay commands, information is displayed for the currently selected access. However, you may also change the access (which, in turn, changes the default) by using these commands along with the access index command. Refer to the `fr a <access n>` command.

`fr display`
Displays the configuration information as entered during the last CFGEDIT session for the currently-selected frame relay access. Note that this also includes any configured PVCs associated with this access.

`fr stats`
Displays the statistics associated with the currently-selected access and DLCI. Refer to *Frame Relay Statistics*, for a list of available statistics and their definitions.

fr clear
Clears the statistics counters associated with the *fr stat* command for the currently selected access and DLCI.

fr clearall
Clears all statistics associated with the *fr stat* command.

fr lmi
Displays information relating to the LMI link on the currently-selected frame relay access, if that access has the layer Management Interface enabled. The following list describes the fields displayed when the FR LMI command is entered.

LMI State
The condition of the LMI link. Possible settings for this item are WAIT FULL STATUS (S1), WAIT T391 TIMEOUT (S2), and WAIT LIV STATUS (S3). The possible settings are defined as follows:

WAIT FULL STATUS
The LMI state entered when the local frame relay software has transmitted a STATUS ENQUIRY message requesting a FULL REPORT STATUS message.

WAIT T391 TIMEOUT
The LMI state entered when the local frame relay software has received a STATUS message from the network in response to a previous STATUS ENQUIRY and has restarted the T391 timer. (The T391 parameter is the configured Link Integrity Verification Timer.)

WAIT LIV STATUS
The LMI state entered when the local frame relay software has transmitted a STATUS ENQUIRY message requesting a LINK INTEGRITY VERIFICATION STATUS message.

LMI Error State
Current LMI alarm condition. When this item is TRUE, the LMI alarm is on, and all associated PVCs are unavailable. When this item is FALSE, the alarm condition is clear.

LMI DLCI
DLCI value associated with the LMI link. This is the DLCI value contained in all LMI messages and varies according to the LMI format in effect. Note that this is not user configurable.

LMI Frames Received
Number of frames received on the LMI link.

Good LMI Frames Received
The number of valid LMI frames received during the last N391 period. This count is reset after each N391 events. (The N391 parameter is the configured Full Status Enquiry Polling Count.)

Errored LMI Frames Received
Number of invalid or errored LMI frames received during the last N391 period. This count is reset when N392 is reached. (The N391 parameter is the configured Full Status Enquiry Polling Count, and the N392 parameter is the configured Error Threshold Count.)

Unknown DLCI list
List of all unknown DLCIs which have been referenced by either STATUS messages or CLLM messages. This information is helpful in finding and solving problems on the Frame Relay

Access. In particular, the DLCI list is maintained within the code to identify all DLCIs for which the network has knowledge, but which are not currently configured. This list is updated when unknown DLCIs are noted through the `LMI FULL REPORT STATUS` messages, or through CLLM messages.

`fr dbg level <level>`
Displays or sets the current debug level for frame relay. If the level parameter is not specified, then the current debug level is displayed. The debug level corresponds to an internal variable that controls how much information is written to the system log as frame relay events occur. Possible settings for this parameter are 0 through 2, with 0 being the least informative and 2 being the most informative.

`fr cong`
Displays the congestion control information for the last 32 Rate Measurement Intervals for the currently selected access and DLCI. It is provided mainly for debug support of frame relay PVCs in order to monitor PVC usage.

IP ROUTING COMMANDS

In order to use the following commands, you must properly configure and initialize IP routing operating mode. In addition, you must enable RIP to use the *ip rip* commands.

The following commands are used to display IP routing information:

`ip addrpool`
Displays the current IP address pool. There are three fields displayed: *address*, *origin*, and *in use:*
- *address*: lists the IP address in the pool
- *origin*: specifies how the IP address has come to be placed into the IP address pool. If the origin is *DHCP*, the IP address was obtained from a *DHCP* server. If the origin is *STATIC*, the IP address was manually configured via CFGEDIT.
- *in use*: specifies whether or not the IP address has been leased to a remote IP host device.

`ip arp`
Displays the current ARP cache table. The IP address, its corresponding MAC address, the type of ARP table (dynamic or static), and the corresponding interface name are displayed.

`ip filter trace <discard> <off>`
Controls the tracing of packets which are discarded as a result of IP filters. Issuing the command without an optional parameter acts as a query to the current state of the trace.

The purpose of this command is to aid in the initial debug of IP filters, providing a list of all discarded packets due to filtering. As such, it should be enabled judiciously, as it has the potential to fill the report log.

`discard`
Enables the tracing of packets which are discarded. When enabled, each discarded packet will cause a log report of the following format:

```
(F) _:_:_:_:#9a00 [IPFILT] <filtername>/condition # at <application point name>/in/out
        {IP} Src: xxx.xxx.xxx.xxx   Dst:   xxx.xxx.xxx.xxx Pr: n
        {UDP} Src: n   Dst: n
```

The first line indicates:

- the number of the condition within that filter which matched the packet and consequently caused a *discard* action,
- the point at which the filter was applied, or a designation of *global*. For an IP network interface, this will be the configured name of the interface. For a device-based filter, this will be the configured device's name.
- *In* or *Out*, corresponding to INPUT or OUTPUT application.

The next lines contain a brief decode of the packet which was discarded. In particular, the packet fields which comprise the packet type comparisons are displayed. The key IP fields are always displayed on one line. If the IP protocol is one of the explicitly recognized values (ICMP, UDP, TCP) the next line will contain a decode of the key fields of that protocol.

off
Disables the trace.

ip ping <host IP address> [timeout /dnnnn]
Sends an ICMP Echo message to a specified host. The parameters for this command are:

host IP address
IP address using dotted decimal notation for the target host.

timeout
Optional parameter that indicates the number of seconds to wait for an ICMP Echo Reply Message. The valid range for the time out value is 1 to 60. The default value is 10.

/dnnnn
Optional parameter that indicates the data size in bytes for the ICMP Echo message. The valid range for the data size value is 0 to 2020. The default value is 0.

Possible Results and their meanings:

`ddd.ddd.ddd.ddd is alive`
The valid ICMP Echo Reply was received from host ddd.ddd.ddd.ddd.

`No response from ddd.ddd.ddd.ddd`
No response was received from the host within the timeout value number of seconds.

ip rip interface
Displays information pertaining to the interface data that is maintained by the IP RIP protocol. The example screen below illustrates the interface information that will be displayed when this command is entered.

```
[System Name]> ip rip interface

Status:                    Active
I/F Type:                  LAN
IP Address:                192.168.1.1
Subnet Mask:               255.255.255.0
Broadcast Address:         192.168.1.255
Transmission:              Version 1
Reception:                 Version 1 or Version 2
Query Response:            Version 1
Version 2 Authentication:  Password

Status:                    Inactive
I/F Type:                  WAN - UNNUMBERED
IP Address:                0.0.0.0 (left.CSX)
Subnet Mask:               N/A
Broadcast Address:         255.255.255.255
Host Route Propagation:    N/A

Status:                    Inactive
I/F Type:                  WAN - NUMBERED
IP Address:                192.168.3.5
Subnet Mask:               255.255.255.0
Broadcast Address:         255.255.255.255
Host Route Propagation:    When host connected
```

ip rip routes

Displays information pertaining to the routing table(s) that are maintained by the IP RIP protocol. The following example screen illustrates the output from this command. Following the table is an explanation of the fields displayed for each route.

```
[System Name]> IP RIP ROUTES

Active Routes
Destination      Subnet-Mask      Next Hop        Mtr P 1/2 TAge
-------------------------------------------------------------------
3.2.0.0          255.255.0.0      0.0.0.0         4   A 1/1 A30
3.3.0.0          255.255.0.0      0.0.0.0         4   A 1/1 A30
192.168.5.0     255.255.255.0    0.0.0.0          0   A 1/1 SN/A
4.4.4.1          255.255.255.255 0.0.0.0          0   A 1/1 HN/A

Inactive Routes
Destination      Subnet-Mask      Next Hop        Mtr P 1/2 TAge
-------------------------------------------------------------------
4.0.0.0          255.0.0.0        0.0.0.0          0 H 0/1 SN/A
```

`Destination`

The route destination. This destination may be a network number, a subnet address, or a host address.

`Subnet-Mask`

The mask used for the destination.

`Next Hop`

The IP address or interface name (for unnumbered interfaces) of the router that is the gateway for the route.

`Mtr`

The cost of using this route (usually the number of hops to the destination).

`P`
The propagation flag, where
`A` = Always propagate
`N` = Do not propagate
`H` = Propagate when Next Hop Device Connected

`1/2`
RIP Version 1/Version 2 visibility flags determine whether or not this route is visible when send the route using RIP 1 or RIP 2, where
`0` = Invisible
`1` = Visible

`T`
The type of route, where
`A` = Active Route, learned via RIP on a LAN interface
`P` = Permanent Route, learned via RIP on a WAN interface
`S` = Static Route, learned via IP Routing Table
`H` = Host Route, created when an IP Host Device is connected

`Age`
The time since the last update was received.

`ip rip send`
Used to send the IP RIP update messages to a particular interface on demand. Example:

```
[System Name]> ip rip send 2.2.2.2

Sending IP RIP Update Message to Network 2.0.0.0
```

`ip rip stats`
Displays global RIP statistics and also statistics for each configured RIP interface. Refer to *RIP Statistics*, for a list of available statistics and their definitions.

`ip route`
Displays the current routing table. Each displayed field for a route entry is as follows:

`Destination`
IP address for the destination network or host.

`Subnet-Mask`
Subnet mask value for the destination network or host. A value of 255.255.255.255 indicates that this entry is for a specific IP host.

`Next Hop`
IP address or device name for the next hop router that provides access to the destination network or the host.

`Metric`
Hop count to the destination network or the host.

`T/P (Type/Protocol)`

`Type`
The destination type is “R” for a remote network or host, and “L” for a locally connected network or host.

`Protocol`
The mechanism used to determine the route. “L” is for local, “I” is icmp, and “R” is for RIP.

`TTL`
Time to Live for this route entry in seconds. This entry will expire after the specified number of seconds. A value of 999 implies that the entry will not expire.

`IF`
The interface Id.

`Age`
The age of the route in seconds.

`ip route <IP address>`
Displays the routing information for the indicated device. The meaning of each displayed field for a route entry is included in the above ***`ip route`*** command explanation.

`ip stats`
Displays the current IP related statistics. Refer to *IP Statistics* for definitions.

IPX ROUTING COMMANDS

IPX routing must be enabled before these commands can be used.

The following commands are used to display IPX routing information:

`ipx ipxwan clear`
Clears IPXWAN statistics.

`ipx ipxwan stats (device)`
Displays system-level IPXWAN statistics when device name not specified:

```
IPXWAN Statistics

Timer Request          =              Timer Response         =
Information Request    =              Information Response   =
Thruput Request        =              Thruput Response       =
Delay Request          =              Delay Response         =
NACK Sent              =              NACK Received          =
Bad Packets            =
```

Displays Negotiation Parameters when device name specified and connected:

```
WAN Statistics for device "xxxx"

Negotiation Parameters:

IPX Network Address =       IPX Node Number =
Telebit Compression =       Protocol        =
WAN Link Delay =
```

ipx diag <host ipx address> [timeout]

Tests device connectivity to specified IPX host by sending out a diag packet. If connection is up, host sends a message in response to this packet to confirm receipt. The parameters for this command are:

`host ipx address`

IPX address for the host, in <network number>:<node number> format. The network number is a hexadecimal number up to eight digits in length. The node number is the host's MAC address. For example, if the assigned network number of "AAAA," and the host has a MAC address of 40AA68965439. For this example, you would enter "AAAA:40AA68965439" for the host IPX address.

`timeout`

Optional parameter that indicates the number of seconds to wait for a reply. The valid range for the time out value is 1 to 60 seconds. The default value is 10.

Note: The *ipx diag* and the *ipx ping* commands both test device connectivity (although both send back different types of responses). However, due to the variety of vendors and equipment available to networks, one command may work with a particular vendor or file server, while the other may not. If you are not experiencing success with *ipx diag*, try *ipx ping*, and vice versa.

ipx ping <host ipx address>

Tests connectivity to the specified IPX device by sending out a data packet (echo message). If connection is up, device responds with an echo reply.

`host ipx address`

IPX address for the host, in <network number>:<node number> format. The network number is a hexadecimal number up to eight digits in length. The node number is the host's MAC address. For example, if the assigned network number of "AAAA," and the host has a MAC address of 40AA68965439. For this example, you would enter "AAAA:40AA68965439" for the host IPX address.

Note: The *ipx ping* and the *ipx diag* commands both test device connectivity (although both send back different types of responses). However, due to the variety of vendors and equipment available to networks, one command may work with a particular vendor or file server, while the other may not. If you are not experiencing success with *ipx ping*, try *ipx diag*, and vice versa.

ipx rip stats

Displays the IPX RIP statistics. Refer to *IPX RIP Statistics* for definitions.

ipx route
Displays the current routing table for the system, including static and learned routes.

ipx route stats
Displays routing table statistics, including maximum number of routes configured, and number of currently-available routes. Refer to *IPX Route Statistics*.

ipx service
Displays the current routes to IPX services for the system, including static and learned routes.

ipx service stats
Displays the current service table statistics, including the maximum number of services this router is configured to handle, and the number of currently-available services. Refer to *IPX Service Statistics*.

ipx sap stats
Displays the IPX SAP statistics. Refer to *IPX SAP Statistics* for definitions.

ipx spoof stats
Displays the IPX spoofing statistics. The IPX spoofing statistics displayed are self-explanatory.

ipx stats
Displays the IPX statistics. Refer to *IPX General Statistics*, for a list of available statistics and their definitions.

ipx trigreq [device]
Generates a triggered RIP/SAP update request to the specified device. You may use this command to initiate an update request to synchronize with the routing database of a particular WAN device.

ipx trigrip stats
Displays the triggered RIP statistics. Refer to *IPX Triggered RIP Statistics*.

ipx trigsap stats
Displays the triggered SAP statistics. Refer to *IPX Triggered SAP Statistics.*

ISDN USAGE COMMANDS

The following commands are used to display and clear ISDN B-channel monitoring information.

isdn usage
Displays the following ISDN B-channel monitoring information:
- The number of ISDN B-channels available.
- The number of ISDN B-channels in use.
- The high-water mark for the number of ISDN B-channels in use.
- The value which the number of ISDN B-channels in use must meet or exceed in order to cause an isdnUsageHigh SNMP trap to be generated by the system.
- The enabled status for the generation of the ISDN usage traps (isdnUsageHigh and isdnUsageNormal).
- The elapsed time since the monitoring of the high-water mark began.

This information can help you determine if additional lines and / or systems are necessary. For example, the high water mark could be compared to the number of ISDN B channels available, taking into consideration the elapsed time. An example output from this command follows:

```
[System Name]> isdn usage

number of ISDN B channels available:  6
number of ISDN B channels in use:     3
high water mark:                      5
isdnBChanUsage trap threshold:        5
generation of ISDN usage traps:       enabled
elapsed time:                         3 days, 4 hrs, 12 min, 38 sec
```

isdn usage clear

Clears the B-channel high-water mark and elapsed time values. The purpose of this command is to allow the user to reset the high-water mark to coincide with changes to the system and / or the network or so that the user can monitor the high-water mark over desired time periods.

LAN COMMANDS

The following commands are used to display current system LAN diagnostic information:

lan stats

Displays the current LAN packet forwarding statistics, including the number of frames received and transmitted from LAN and WAN connections. Refer to *LAN Statistics*, for a list of available statistics and their definitions.

lan stat clear

Clears the current LAN packet forwarding statistics.

lan test

Transmits a test message onto the LAN and test for proper LAN connections. If the transmit is successful, the following message will be displayed:

`LAN port <port #> Transmit was successful`

If the transmit fails, refer to the section titled *LAN Connections* to determine the reason for the failure.

LOG COMMANDS

The following commands control the report logging feature for the system's subsystems.

log cdr display

Displays the local call detail recording report log.

log cdr erase

Erases the local call detail recording log report.

log cdr write

Writes the local CDR log to disk. The file is written to the \LOG directory. The file name is "CDR_LOG". The file extension is .1, .2, and so on up to .10. The file extension cycles through the extension values with each write command, similar to the current report log file and status log file, so that the ten most recent versions of the CDR log are available on the system disk.

PACKET CAPTURE COMMANDS

In many applications, it is often desirable to monitor incoming LAN data. The *pkt* commands will allow you to capture, display, save, and load bridged or routed data packets.

You must configure the terminal setting the same for Telnet and the terminal emulation package. To do this, use the *term set* command.

Note: Packet capture commands are available for both local and remote (Telnet) connections.

The following diagnostic packet commands are available:

pkt [on/off]
Enables or disables the Packet Capture feature.

pkt capture [all/idle/reqd/pend/actv/none]
Specifies which packets will be captured by the Packet Capture feature. A definition of each possible parameter follows.

all
All packets will be captured.

none
No packets will be captured.

reqd
Only packets causing a connection to be requested will be captured.

pend
Only packets received while a requested connection is pending will be captured.

idle
Only packets not causing a connection to be requested will be captured. This could be caused by the destination site not being in the Initiate Connection List, or by the route not being in the IP Routing Table.

The *pkt capture* command allows multiple connection modes to be specified on a single command line. For example, the command:

```
pkt capture reqd pend
```

captures only packets that cause a connection to be requested and packets that were received before the connection became active.

pkt load <filename>
Loads previously saved Packet Capture file into memory.

pkt save <filename>
Saves captured packets to a disk file. Full path names are allowed, for example: `A:MYPKT.DAT`.

pkt display

Displays captured packets that have been collected via *pkt on* or via *pkt load*. Note that this command is not supported for a Telnet session.

The following is an example *pkt display* screen:

```
Num   Time(mSEC) Len   Dest Addr              Source Addr            Type Conn

0001 0000000000 0064 00004440259C          02608C4C0EAD           8137 PEND
0002 0000000000 0064 00004440259C          02608C4C0EAD           8137 PEND
0003 0000000000 0064 00AA00302D25          02608C4C0EAD           8137 PEND
0004 0000000000 0064 00AA00302D25          02608C4C0EAD           8137 PEND
0005 0000001980 0064 00004440259C          02608C4C0EAD           8137 PEND
0006 0000001980 0064 00004440259C          02608C4C0EAD           8137 PEND
0007 0000001980 0064 00AA00302D25          02608C4C0EAD           8137 PEND
0008 0000001980 0064 00AA00302D25          02608C4C0EAD           8137 PEND
0009 0000003190 0028 001.001.001.001       001.001.001.001        IP    ACTV
0010 0000003190 0028 001.001.001.001       001.001.001.001        IP    ACTV
0011 0000003960 0064 00004440259C          02608C4C0EAD           8137 PEND
0012 0000003960 0064 00004440259C          02608C4C0EAD           8137 PEND
0013 0000003960 0064 00AA00302D25          02608C4C0EAD           8137 PEND
0014 0000003960 0064 00AA00302D25          02608C4C0EAD           8137 PEND
0015 0000004670 0064 FFFFFFFFFFFF          02608C4C0EAD           8137 PEND
0016 0000004670 0064 FFFFFFFFFFFF          02608C4C0EAD           8137 PEND



                   Hit <ESC> to Exit or <F1> for Help
```

It is possible to display packet details for a specific packet. To do so, use the keyboard's arrow keys to move the cursor to the desired packet number (on the "pkt display" screen); then press <return> to display detailed information for that packet. The following screens are example packet detail screens for various packet types.

NOVELL NetWare® Packet Detail Screen (Bridged Packet)

```
Packet Number      Received at Time     Packet Length
      0015            0000004670 mSEC        0064
 Destination Address    Source Address
     FFFFFFFFFFFF          02608C4C0EAD
 EtherNet Type is 8137,   Novell IPX
 Check Sum   Packet Length   Packet Type   Transport Ctl
    FFFF        0x0028         00,???          00
                  Network          Node       Socket
 Destination    0000AAA1      FFFFFFFFFFFF    0453 RIP
 Source         0000AAA1      02608C4C0EAD    0453 RIP

 Routing Information Protocol Socket Header

00 02 00 00 FF FD 00 01 00 02                    ..........


               Hit Escape to EXIT Packet Details
```

Banyan Vines Packet Detail Screen (Bridged Packet)

```
Packet Number      Received at Time     Packet Length
      0021             0000022190 mSEC        0060
 Destination Address            Source Address
     FFFFFFFFFFFF                 02608C9BED38
 EtherNet Type is 0BAD,   VINES IP
 Check Sum        Packet Length       Protocol Type
    D75D            0x001A              04, ARP
 Transport Control        Hop Count
        0                      0
 Dest Network Dest SubNet   Source Network Source SubNet
   FFFFFFFF       FFFF          00000000         0x0000

 Packet Type     Network Number      Subnetwork Number
     Query           126697007              0x9183


                     Hit Escape to EXIT Packet Details
```

IP Datagram Detail Screen (Routed Datagram)

```
Packet Number      Received at Time     Packet Length
      0009             0000003190 mSEC        0028
 Destination Address    Source Address
     001.001.001.001       001.001.001.001

45 00 1C 00 01 00 00 00 40 01 76 DD 01 01 01 01    E.......@.v.....
01 01 01 01 08 00 C3 ED 34 12 00 00               ........4...




                     Hit Escape to EXIT Packet Details
```

While the “pkt display” is displayed on your monitor, you can display the following help screen by entering “**?**”:

```
ESC   - Exit Menu
‘u’   - Previous Menu
‘d’   - Next Menu
‘h’   - Top of Packet List
‘e’   - End of Packet List
Enter - Display Packet Details
‘t’   - Time Menu
‘m’   - Marks Packet as Start Time
Cursor- to select an entry

               Hit any key to exit Help
```

The time menu that is displayed when “*t*” is entered will enable you to toggle the time increment to be in either Sec (seconds), mSec (milliseconds), or tSec (deciseconds).

When the packet marking option is used, all packet times will be displayed relative to that marked packet. To mark a packet, use the arrow keys to move the cursor to the selected packet number, then press "*m*" The time for that packet will be set to 0. All packets received before that packet will have negative time values. All packets received after that marked packet will have progressively higher positive time values.

RADIUS COMMANDS

The following console commands may be used to diagnose problems with:

- connections to the off-node RADIUS authentication server
- CyberSWITCH configuration
- authentication server device database entries

radius chap

Attempts an authentication session using CHAP. The following is an example display of the screen.

```
[System Name]>radius chap

Enter the device name (<RET> to abort)? doe

Enter secret (<RET> to abort)? secret123

Send Radius Authentication Request... Please wait
Authentication Successful...

 Device-Name:          doe
 Framed-Address:150.001.001.001
 Phone-Number: 1-800-555-1212
 Phone-Subaddress:3456
 Caller-Id:            2340823-098
 Framed-Data-Rate:64KB
 Framed-Protocol:PPP/IP
```

radius ifname

Attempts an authentication session using I/F NAME LOOKUP. The following is an example display of the screen.

```
[System Name]>radius ifname

INTERFACE NAME to determine route for (<RET> to abort)? left.CSX

Send Radius Authentication Request... Please wait
Authentication Successful...

 Device-Name:         left.CSX
 Framed-Address:      128.111.1.3
 Phone-Number:        18005551212
 Framed-Data-Rate:    64KB
 Framed-Protocol:     PPP/IP
 Framed-Route: 3.0.0.0 255.0.0.0 128.111.1.3 2 RAP(RIP-Always Propagate)
```

radius iphost

Attempts an authentication session using the IP Host resolution. The following is an example display of the screen.

```
[System Name]>radius iphost

IP HOST id of the Host logging in (<RET> to abort)? 811145678234567812345678

Send Radius Authentication Request... Please wait
[AUTH] Warning code: 0002 Missing required attribute from server.

Framed-Data-Rate:   64KB

 Missing attribute: Device-Name
```

radius ipres

Attempts an authentication session using the IP resolution. The following is an example display of the screen.

```
[System Name]>radius ipres

IP Address of the Host logging in (<RET> to abort)? 19.63.4.5

Send Radius Authentication Request... Please wait
[AUTH] Warning code: 0001 Timeout.
```

radius macres

Attempts an authentication session using the MAC resolution. The following is an example display of the screen.

```
[System Name]>radius macres

MAC Address of the Host logging in (<RET> to abort)? 0ab34252d546

Enter password? password123

Send Radius Authentication Request... Please wait
[AUTH] Warning code: 0002 Missing required attribute from server.

 Caller-Id:           2340823-098
 Framed-Data-Rate:    64KB

 Missing attribute:   Device-Name
```

radius pap

Attempts an authentication session using PAP. The following is an example display of the screen.

```
[System Name]>radius pap

Enter the device name (<RET> to abort)? doe

Enter password (<RET> to abort)? password123

Send Radius Authentication Request... Please wait
Authentication Rejected...
```

radius route

Attempts an authentication session using ROUTE LOOKUP. The following is an example display of the screen.

```
[System Name]>radius route

IP Address to determine route for (<RET> to abort)? 3.3.3.3

Send Radius Authentication Request... Please wait
Authentication Successful...

 Device-Name:        left.CSX
 Framed-Address:     128.111.1.3
 Phone-Number:       18005551212
 Framed-Data-Rate:   64KB
 Framed-Protocol:    PPP/IP
 Framed-Route:3.0.0.0 255.0.0.0 128.111.1.3 2 RAP(RIP-Always Propagate)
```

SERIAL INTERFACE COMMANDS

These commands are available only when you have a serial interface card (V.35 or RS232) properly installed:

ser <#> stats
Displays the current serial interface statistics for each line (V.35 or RS232) attached to the card in the specified slot #. Refer to *Serial Interface Statistics* for a list and definition of these statistics.

ser <#> clear
Clears the current serial interface statistics for each line (V.35 or RS232) attached to the card in slot #.

ser <#> signal
Displays the current state of the input signals for each line (V.35 or RS232) attached to the card in slot #. A value of ***0*** indicates an *inactive* signal, and a value of ***1*** indicates an *active* signal.

SNMP COMMANDS

When the SNMP Agent is enabled on the CyberSWITCH, the following command is available:

snmp stats
Displays the current SNMP related statistics. Refer to *SNMP Statistics*, for a list of available statistics and their definitions.

SPANNING TREE COMMANDS

Spanning Tree protocol is supported only on the two port Ethernet-2 adapter card. The Ethernet-1 adapter card does not support Spanning Tree protocol, but does have access to the "BRIDGE AGE TIME" Spanning Tree Information.

When Spanning Tree protocol is enabled on the CyberSWITCH, the following commands are available:

br stpport <port #>
Displays Spanning Tree port information for the specified port number (either "1" or "2").

br stpbrdg
Displays Spanning Tree bridge information.

SPANNING TREE PORT INFORMATION

When Spanning Tree protocol is enabled on the CyberSWITCH, the following Spanning Tree Port Information is available for each LAN port on the system. This information is generated by issuing the *br stpport <port #>* Spanning Tree command.

`Port Priority`
The configured priority for this port.

`State`
The current state of the port. Possible values are; DISABLED, BLOCKING, LISTENING, LEARNING, and FORWARDING.

`Path Cost`
The configured path cost for this port.

`Designated Cost`
The path cost to the root bridge for this port.

`Desig Root Addr`
The MAC address for the root bridge.

`Desig Root Prior`
The bridge priority for the root bridge.

`Desig Brdg Addr`
The MAC address for the designated bridge.

`Desig Brdg Prior`
The bridge priority for the designated bridge.

`Desig Port Number`
The port number on the designated bridge.

`Desig Port Prior`
The port priority for the port on the designated bridge.

`Topology Chng Ack`
The topology change acknowledgment value to be transmitted in the next Spanning Tree message.

`Config Pending`
The flag that indicates that the system is waiting to transmit a configuration Spanning Tree message.

SPANNING TREE BRIDGE INFORMATION

When Spanning Tree protocol is enabled on the CyberSWITCH, the following Spanning Tree Bridge Information is available. This information is generated by issuing the *`br stpbrdg`* Spanning Tree command.

`Bridge Address`
The MAC address of the CyberSWITCH.

`Bridge Priority`
The configured priority for the CyberSWITCH.

`Root Address`
The MAC address of the root bridge.

`Root Priority`
The bridge priority of the root bridge.

`Root Path Cost`
The path cost to the root bridge.

`Root Port Num`
The port number on the CyberSWITCH that offers the lowest cost path to the root bridge. This is set to 0 if the system is the root bridge.

`Root Port Prior`
The port priority of the Root Port Number.

`Max Age`
The maximum time (in tenths of a second) allowed without receiving a Spanning Tree message from the root bridge.

`Hello Time`
The time interval (in tenths of a second) between the transmission of configuration Spanning Tree messages. This is only used when the system is the root bridge.

`Fwd Delay Time`
The time (in tenths of a second) spent in the LISTENING and LEARNING state.

`Bridge Max Age`
The configured maximum age-time for the system. This is used when the system is the root bridge.

`Brdg Hello Time`
The configured hello time interval for this system. Used when the system is the root bridge.

`Br Fwd Delay`
The configured forward delay time for the system. Used when the system is the root bridge.

`Tplgy Chng Time`
The time period (in tenths of a second) for sending configuration Spanning Tree messages that have the topology change flag set. Only used when the system is the root bridge.

`Tplgy Ch Detect`
A flag that is set to "TRUE" when the system detects a topology change.

`Topology Change`
A flag that sets the topology change flag in configuration Spanning Tree messages that are transmitted. Used when the system is the root bridge.

`Aging Time`
The time period (in tenths of a second) used by the system to age unused entries out of the address table.

`Default Age Time`
The configured aging time the system uses.

`STP Enabled`
A flag that is set to “1” if the Spanning Tree protocol is enabled.

TCP COMMANDS

TCP (Transmit Control Protocol) provides a connection-oriented reliable communication for delivery of packets to a remote or on-node device. When the IP feature is enabled, the following TCP commands are available:

`tcp conns`
Display the current TCP connection status with the following format:

`lport`
The local port number for this TCP connection.

`fhost`
The remote IP address for this TCP connection.

`fport`
The remote port number for this TCP connection.

`window (l/r)`
The current receive windows for the local and remote ends of this TCP connection.

`tstate`
The current state of this TCP connection.

`outq (s/u)`
The number of bytes that has been sent but not acknowledged yet and the number of bytes in the output queue that has not been sent on this TCP connection.

`tcp stats`
Displays the current system TCP related statistics. Refer to *TCP Statistics*, for a list of available statistics and their definitions.

TELNET COMMANDS

These commands are Telnet client console commands. These commands provide tools for you when you are using the system as a Telnet client. As a Telnet client, the CyberSWITCH can then be used to Telnet into another CyberSWITCH to perform system maintenance, for example, updating configuration information. These commands are not needed for a Telnet session as a rule, but may be beneficial for some users. For more information regarding the system's Telnet client feature, refer to the *Telnet* section of the *Remote System Management* chapter.

telnet ?

Displays the help screen for the ***telnet*** command. The help screen provides the syntax for the command described below.

telnet <ip-address> [port number]

Begins a Telnet session for the Telnet host at the indicated IP address. The port number is an optional parameter that can be used to specify the destination port number. Include this parameter if you wish to connect to a port other than the default port number, 23.

telnet

The telnet command used with no arguments, as opposed to the above command, puts you in the Telnet command mode. Once you are in the Telnet command mode, the following commands are then available.

close

Used to close the current Telnet connection to a target host.

exit

Closes the current Telnet session. If a connection exists to a target host, it is gracefully closed.

open

Used to establish a Telnet session with a target host. You can enter the IP address of the target host, and optionally, the remote port number, to connect to. If no remote port number is specified, the default Telnet port is used (23). The valid range for port number is 1 to 65535. The IP address specified is verified for proper format.

If a Telnet session is successfully initiated as a result of the ***open*** command, a screen similar to the following will be displayed:

```
telnet>open 204.157.42.150
Trying 204.157.42.150...
Connected to 204.157.42.150.
Escape character is '^]'.
```

If an IP address (and port) are not specified on the "open" command line, you will be prompted for the target host's IP address.

send [send parameter]

Used to send special Telnet control functions to the currently connected target host. A connection must be fully established before you can send anything. If no parameters are specified on the ***send*** command line, the following help message is displayed:

```
[System Name]>send
 Available send commands:
    ayt      - Send "Are You There?" request to server
    break    - Send "Break" request to server.
    escape   - Send current "escape" character to server.
    synch    - Send "Synch" signal to server.
    ?        - Display this help information.
```

The possible send parameters are defined as follows:

send ayt

The *send ayt* command sends the Telnet command function for “Are You There?” to the target host. This can be used to determine whether or not the target host is still responding. The target host is not required to respond to “are you there?" requests, but if it does, you should see something like the following:

```
[System Name]>send ayt

[Yes]
```

send break

The “send break” command sends the Telnet command function for “BREAK” to the target host. This can be used to interrupt the current command in progress on the target host. For example: If the target host is currently streaming out a large directory listing, you can issue the *send break* command to terminate the directory command. Once again, this functionality is dependent upon the target host’s processing of the “BREAK” control function.

send escape

The *send escape* command sends the current escape character for the Telnet session. If the connection between the local terminal and the remote server is made up of more than 1 individual Telnet connection, this command may be used to “escape” into command mode of one of the intermediate Telnet connections.

send synch

The *send synch* command sends the Telnet “SYNCH” signal (the “DM” control function as TCP urgent data) to the target host. This command may be useful when trying correct a situation where the target host appears to be in an atypical state of processing.

set

The *set* command can be used to set certain operating parameters for the current Telnet session. The format of the *set* command is *set <name> <value>*; where <*name*> is the parameter to be set, and <*value*> is what the parameter should be set equal to.

If no parameters are specified on the “set” command line (or if “set?” is entered), the following help message is displayed:

```
[System Name]>set
 Available set commands:
    escape - Character used to escape back to TELNET command mode.
    ?      - Display this help information.
```

The *set escape* command can be used to change the "escape" character for the current Telnet session. This command may be useful when a device is connected to a target host, using several different Telnet connections. By changing the escape character to a value other than the default (<CTRL>), the user can return to Telnet "command" mode for a particular session.

Typically, Telnet "escape" characters have the form '<CTRL><char>' (i.e., the CTRL key + some other key must be pressed). The <value> parameter for the "set escape" command may have any of the following values:

- <CTRL><char>, where <char> is in the range of ASCII 'A' to ASCII '_'
- <CTRL><char>, where <char> is in the range of ASCII 'a' to ASCII 'z' (note that lower case letters are converted to upper case before they are used)
- <char>, where <char> is in the range of ASCII '!' to ASCII '~'

To specify the <CTRL> key in the *set escape* command, use the '>' character. The following is an example of setting the escape character equal to '<CTRL> P':

```
[System Name]>set escape ^P
Escape character is '^P'.
```

status

The *status* command can be used to interrogate information about the current Telnet session.

toggle

The *toggle* command can be used to set various operating parameters for the current Telnet session. Currently, the only parameter available is *debug*.

If no parameters are specified on the *toggle* command line (or if *toggle ?* is entered), the following help message is displayed:

```
[System Name]>toggle
 Available toggle commands:
    debug - Turn TELNET debug mode on or off.
    ?     - Display this help information.
```

The toggle debug command allows you to turn the Telnet debug mode on or off. If the debug mode is turned on, messages beginning with "[TELNET-C]" may appear in the system log file. Most users will not find these messages helpful. If you have difficulty with the system Telnet client feature, we suggest you call your Distributor or Customer Support.

TERMINAL COMMANDS

The CyberSWITCH supports two terminal types: vt100 and ANSI. When a Telnet connection is established, the system attempts to negotiate the terminal type. When the negotiation fails, the system sets the terminal type to vt100.

To successfully issue the *pkt display*, *semi perm*, and *mc* commands, you must have the terminal type set identically for both the Telnet emulator and the terminal emulation. To do this, use the *term set* command.

The following commands are used to display the terminal type currently in use or to set the terminal type.

term
Displays the terminal type name.

term set <terminal type>
Allows you to set the terminal type. You may set the terminal type to either vt100 or ANSI.

TFTP COMMANDS

The TFTP feature and its commands are only available when IP routing is enabled. The TFTP feature and file access are enabled by default when the system software is installed. Using the Manage Mode, configuration changes may be made that will limit file access. The following TFTP commands are available:

tftp get
Allows you to perform the "TFTP GET" operation locally from the console through the TFTP Client function. The following is an example display of a TFTP GET screen.

```
> TFTP GET

>IP Address of the Host containing the file
(<RET> to abort)? 19.233.45.33

>Enter the name of the local file to write (including the full path)?
(<RET> to abort)? \config\config.nei

>Enter the name of the remote file (including the full path)
(<RET> for same as local)? <RET>

Enter the mode (BIN [binary] or ASC [ascii])
<RET> for ascii? bin

Receiving File... Please wait
File Transfer Complete...
```

tftp kill <session Id>
Allows you to kill a TFTP session. The session Id must be included in this command. To obtain the session Id, issue the *tftp session* command which displays the TFTP session information.

tftp put
Allows you to perform the TFTP PUT operation locally from the console through the TFTP Client function. The following is an example display of a TFTP PUT screen.

```
> TFTP PUT

>IP Address of the Host to receive the file
(<RET> to abort)? 19.233.45.33

>Enter the name of the local file to send (including the full path)
(<RET> to abort)? \config\config.nei

>Enter the name for the remote file (including the full path)
(<RET> for same as local)? <RET>

Enter the mode (BIN [binary] or ASC [ascii])
<RET> for ascii? bin

Sending File... Please wait
File Transfer Complete...
```

tftp session

Displays the TFTP session information of active TFTP sessions. To get detailed information on a specific session, enter the session's Id number when prompted. You can not display the session information for a TFTP session that has terminated. The following screen illustrates the use of this command.

```
> TFTP SESSION

Id Sess-Id Local file    Type/Mode   Bytes Xmit Retries
-------------------------------------------------------
 1        5 temp.txt      Client/Put       12752        1
 2        6 tmp           Server/Get         423        0
 3        7 text.txt      Server/Put        8481        0

Select the ID of the TFTP Session to display or <RET> to cancel? 2

TFTP Session ID:     6
Type:                Server
Mode:                Get
Local Address:       190.5.6.8   (UDP Port: 5001)
Local File:          c:\tmp
Remote Address:      190.5.6.11 (UDP Port: 5011)
Remote File:         N/A
Transfer Mode:       netascii
Bytes Transferred:   935
Bytes Remaining:     1145723
Total Retries:       0
```

tftp stats

Displays the current TFTP related statistics. Refer to *TFTP Statistics*, for a list of available statistics and their definitions.

TRACE COMMANDS

Note: For an explanation regarding the output resulting from the family of trace commands, refer to the *Trace Messages* chapter.

The following commands are used to enable and disable trace reporting information:

trace ipxwan [on/off]
Enables or disables the IPXWAN tracing option, which tracks all packets which are received or sent out using IPXWAN protocol, and places this information in the system log. To display the log file, issue the *dr* command. This option is initially disabled.

trace lapb [on/off]
Enables or disables the LAPB data link information packet tracing option. This feature displays up to 15 octets of the packet. To display the log file, issue the *dr* console command. This option is initially disabled.

trace [on/off]
Enable or disables the call trace information reports. If enabled, you can then view the logged call trace information by issuing the *dr* command. For details on call trace messages, refer to the chapter titled *Trace Messages*.

trace ppp [on/off]
Enables or disables the tracing of incoming and outgoing PPP packets. If enabled, you can view the trace PPP information by issuing the *dr* command.

trace x25 [on/off]
Enables or disables the X.25 packet tracing option. This feature displays up to 15 octets of the packet. To display the log file, issue the *dr* console command. This option is initially disabled.

wan fr-ietf trace [on/off] [in/out] [device/fr_accessname_dlci] [prot]
Enables or disables the tracing of incoming and out going frame relay IETF packets. This feature displays the direction of the packet, the device or PVC name, the line protocol, and up to 15 octets of the packet. To display the log file, issue the *dr* console command. This option is initially disabled.

UDP COMMANDS

UDP (User Datagram Protocol) provides a datagram mode of communication for delivery of packets to a remote or on-node device. When the system's IP operating mode is enabled, the following UDP commands are available:

udp conns
Displays the current UDP connection status.

udp stats
Displays the current system UDP statistics. Refer to *UDP Statistics* for definitions.

USER LEVEL SECURITY COMMANDS

The following console commands are available to provide information on the authentication servers for user level security. They may be used to diagnose the following problems with:

- connections to an off-node authentication server
- CyberSWITCH configuration
- authentication server user database entries

sentry log
This command acts as a toggle switch, enabling or disabling user authentication rejection messages. If enabled, authentication rejection messages (identifying users who generated the messages) are written to the log file. To display the log file, issue the *dr* console command. This option is initially disabled.

sentry status
Displays current Sentry status. This includes whether or not trace is enabled, as well as the status and port number of each authentication server on the system.

sentry tacacs
Attempts an authentication session using TACACS. The system will report whether the authentication attempted was successful or rejected.

sentry radius
Attempts an authentication session using RADIUS. The system will report whether the authentication attempted was successful or rejected.

sentry ace
Attempts an authentication session using ACE. The system will report whether the authentication attempted was successful or rejected. Upon initial configuration of ACE, this command also establishes a secret for the CyberSWITCH and the ACE server. This secret is necessary for future authentication negotiations.

WAN COMMANDS

The following commands are used to display current system WAN diagnostic information:

wan fr-ietf stats [device/fr_accessname_dlci] [prot]
Displays the current frame relay IETF related statistics. Refer to *WAN FR_IETF Statistics*, for a list of available statistics and their definitions.

wan l1p
This group of commands provide primary rate interface layer 1 information. *wan l1p* is the prefix for all commands in this group. The syntax and definition for each wan l1p command follows. (Note that for each command, you must include the slot number of the PRI adapter.)

wan l1p alarm display <slot #>
Displays any alarms currently being received by the primary rate layer 1. Because many incoming alarms are qualified for several seconds before being declared, this display may indicate an alarm when layer 1 has not been declared down. The following table provides the possible alarms and their meanings.

Alarm Type	*Alarm Meaning*
Loss of Signal (Red)	An all zero signal (or complete lack of signal).
Loss of Frame (Red)	A signal which does not match the configured framing mode (for example, ESF).
AIS (Blue)	An unframed all one signal.
RAI (Yellow)	A Remote Alarm Indication signal.

wan l1p error [display or clear] <slot #>
When ***display*** is used, this command displays the PRI layer 1 error counters. Refer to *Layer 1 PRI Error Statistics* for a list of available statistics and their definitions.

wan l1p loopback status <slot #>
Displays the current status of all loopbacks. (Refer to the following two "loop" commands.

wan l1p lcl_loop [disable or enable] <slot #>
Disables or enables a local loopback. When enabled, this loopback feeds the PRI adapters's transmit signal back to the PRI adapters's receive signal. It is useful in checking for problems in the PRI adapter itself.

wan l1p rem_loop [disable or enable] <slot #>
Disables or enables a remote loopback. When enabled, this loopback feeds the network's transmit back to the network's receive. This is useful for allowing switch personnel to test the entire connection from the switch to the PRI adapter and back.

wan l1p stats [display or clear] <slot #>
When ***display*** is used, this command displays the PRI layer 1 statistics. Two sets of statistics are provided: the specific PRI interface statistics, and layer 1 general statistics. Refer to *WAN L1P Statistics* for a list of available statistics and their definitions.

When ***clear*** is used, these statistics are cleared.

wan stats
Displays the current WAN statistics. Refer to *WAN Statistics* for a list of available statistics and their definitions.

X.25 COMMANDS

The following commands are used to display information concerning both the status and traffic statistics of a particular X.25 connection. A command is also available to allow the X.25 and LAPB packet tracing options to be enabled or disabled.

trace lapb [on/off]
Enables or disables the LAPB data link information packet tracing option. This feature displays up to 15 octets of the packet. To display the log file, issue the ***dr*** console command. This option is initially disabled.

trace x25 [on/off]
Enables or disables the X.25 packet tracing option. This feature displays up to 15 octets of the packet. To display the log file, issue the *dr* console command. This option is initially disabled.

x25 clear
Clears the statistics counters associated with the *x25 stat* command for the currently selected access and LCN.

x25 clearall
Clears all statistics associated with the *x25 stat* command for the currently selected access and LCN.

x25 display [access name]
Displays the configuration for the default X.25 access if no access name is specified. If an access name is specified, the configuration for that access is displayed. Note that this also includes any configuration information of any PVCs associated with this access.

x25 l <LCN "m">
The "l" option will set the Logical Channel Number (LCN) index specified by "m" as the default LCN for subsequent commands entered without an explicit LCN specifier. LCN "m" will remain the default LCN until the default is changed through reissuing the *x25 l <lcn "m">* command.

x25 a <access name>
The "a" option will set the access name specified by *<access name>* as the default access for subsequent commands entered without an explicit access specifier. This access name will remain the current access, until it is changed through issuing another *x25 a <access name>* command.

Note: This command may be used with all other x25 commands. For example, *x25 a acc1 vc* would be a valid command, changing the default X.25 access to "acc1", and would display virtual circuit information for the X.25 access named "acc1".

x25 stats
Displays the statistics associated with the X.25 access. Refer to *X.25 Statistics* for a list of available statistics and their definitions.

x25 vc <LCN>
Sets the default virtual circuit (VC) by specifying the VC's LCN. This VC will be the default for subsequent *vc* commands. This VC will remain the default VC, until it is changed through issuing another *x25 vc <LCN>* command.

x25 vc active
Displays a list of all active VCs for the default X.25 access and LCN.

x25 vc clear
Clears the statistics for the default VC.

x25 vc stats
Displays the statistics for the default VC. Refer to *X.25 Statistics* for a list of available statistics and their definitions.

SYSTEM STATISTICS

OVERVIEW

Statistics can either be generated by issuing the *ds* command to display the set of statistics known as the System Statistics, or by issuing a specific command to display statistics in a specific category.

In addition to using the *ds* command to display the system statistics, they are also automatically written to a statistics log every 30 minutes. The statistics are stored in the following location:

Directory: `\log`
File Name: `stat_log.nn`
("`nn`" is an integer that is incremented each time a new file is written.

You may display these log files using DOS commands. For example, to display the statistics log with the extension of 10, you could enter the following command at the DOS prompt:

C:\> type \log\stat_log.10 | more

Note: The log extensions are revolving numbers. When your machine first begins operating, the files will progress from the .01 extension to the .10 extension. After that time, the oldest report (.01) would be replaced with the latest report. To make sure you are viewing the log file you wish to see, issue a DOS dir command of the log directory to display the time that each log file was written to disk.

The first set of statistics, System Statistics, are arranged by function. These are:

- connectivity statistics
- call restriction statistics
- call statistics
- throughput monitoring statistics

The rest of the statistics are arranged in alphabetical order. These statistics pertain to specific features. The statistics you choose to display will depend on which system options you have enabled. These statistics provide valuable information.

CONNECTIVITY STATISTICS

You can access Network Connectivity statistics by issuing the *ds* console command.

`ISDN_Re-try`
Retry count for re-establishing the data link after it fails.

`ID_Re-try`
Retry count for exchanging identification messages with a remote CyberSWITCH.

`ID_Fail`
Failure count for exchanging identification messages with a remote CyberSWITCH.

`WAN_Reset`
Reset count for the resetting of the WAN adapters.

CALL RESTRICTION STATISTICS

The system keeps a tally of the following Call Restriction statistics. These statistics can be compared to the limits you have configured. These statistics can be displayed by issuing the *cr stats* or the *ds* command at the administration console.

`call minutes (day)`
The total call minutes that have been logged for the day.

`call minutes (month)`
The total call minutes that have been logged for the month.

`calls (day)`
The total number of calls that have been made for the day.

`calls (month)`
The total number of calls that have been made for the month.

CALL STATISTICS

You can access these statistics by issuing the *ds* console command.

`Initiated`
The number of switched calls initiated.

`Completed`
The number of switched call attempts that were completed successfully.

`Re-tries`
The number of switched call retries.

`NoResource`
The number of switched call requests that could not be completed because of a call resource shortage. This could be a shortage on the requesting side or the receiving side.

THROUGHPUT MONITORING STATISTICS

You can access these statistics by issuing the *ds* console command.

`Overload`
The number of bandwidth overload conditions.

`Underload`
The number of bandwidth underload conditions.

`Idle`
The number of idle conditions that caused the last switched connection to be disconnected.

APPLETALK STATISTICS

You may display AppleTalk protocol statistics (subdivided into six subgroups) and AppleTalk port statistics.

You can display all six subgroups of the AppleTalk protocol statistics by issuing the ***atalk stats*** command, or you can display the individual subgroups by adding an extra variable to the ***atalk stats*** command.

You can display the AppleTalk port statistics by issuing the ***atalk port stats*** console command. A definition of these statistics begin on page 633.

APPLETALK PROTOCOL STATISTICS

The six subgroups of AppleTalk protocol statistics are:

- AppleTalk DDP Statistics
- AppleTalk AEP Statistics
- AppleTalk RTMP Statistics
- AppleTalk ZIP Statistics
- AppleTalk NBP Statistics
- AppleTalk ATP Statistics

We include a section of available statistics and their definitions for each subgroup.

APPLETALK DATA DELIVERY PROTOCOL (DDP) STATISTICS

You can display this subgroup of AppleTalk statistics by issuing the ***atalk stats ddp*** console command.

`ddpOutRequests`
The total number of DDP datagrams which were supplied to DDP by local DDP clients in requests for transmission. Note that this counter does not include any datagrams counted in ddpForwRequests.

`ddpOutShorts`
The total number of short DDP datagrams which were transmitted from this system.

`ddpOutLongs`
The total number of long DDP datagrams which were transmitted from this system.

`ddpInReceives`
The total number of input datagrams received by DDP, including those received in error.

`ddpInLocalDatagrams`
The total number of input DDP datagrams for which this system was their final DDP destination.

`ddpNoPrtclHandlers`
The total number of DDP datagrams addressed to this system that were addressed to an upper layer protocol for which no protocol handler existed.

`ddpTooShortErrors`
The total number of input DDP datagrams dropped because the received data length was less than the data length specified in the DDP header or the received data length was less than the length of the expected DDP header.

`ddpTooLongErrors`
The total number of input DDP datagrams dropped because they exceeded the maximum DDP datagram size.

`ddpShortDDPErrors`
The total number of input DDP datagrams dropped because this entity was not their final destination and their type was short DDP.

`ddpChecksumErrors`
The total number of input DDP datagrams for which this DDP entity was their final destination, and which were dropped because of a checksum error.

`ddpFwdingTblOverflws`
The number of times this system attempted to add an entry to the forwarding table but failed due to overflow.

`ddpForwRequests`
The number of input datagrams for which this system was not their final DDP destination, as a result of which an attempt was made to find a route to forward them to that final destination.

`ddpOutNoRoutes`
The total number of DDP datagrams dropped because a route could not be found to their final destination.

`ddpBroadcastErrors`
The total number of input DDP datagrams dropped because this system was not their final destination and they were addressed to the link level broadcast.

`ddpHopCountErrors`
The total number of input DDP datagrams dropped because this system was not their final destination and their hop count would exceed 15.

APPLETALK ECHO PROTOCOL (AEP) STATISTICS

You can display this subgroup of AppleTalk statistics by issuing the *`atalk stats echo`* console command.

`atechoRequests`
The number of AppleTalk Echo requests received.

`atechoReplies`
The number of AppleTalk Echo replies sent.

`atechoOutRequests`
The count of AppleTalk Echo requests sent.

`atechoInReplies`
The count of AppleTalk Echo replies received.

APPLETALK ROUTING TABLE MAINTENANCE PROTOCOL (RTMP) STATISTICS

You can display this subgroup of AppleTalk statistics by issuing the ***`atalk stats rtmp`*** console command.

`rtmpInDataPkts`
A count of the number of good RTMP data packets received by this system.

`rtmpOutDataPkts`
A count of the number of RTMP packets sent by this system.

`rtmpInRequestPkts`
A count of the number of good RTMP Request packets received by this system.

`rtmpNextIREqlChanges`
A count of the number of times RTMP changes the Next Internet Router in a routing entry because the hop count advertised in a routing table was equal to the current hop count for a particular network.

`rtmpNextIRLesChanges`
A count of the number of times RTMP changes the Next Internet Router in a routing entry because the hop count advertised in a routing table was less than the current hop count for a particular network.

`rtmpRouteDeletes`
A count of the number of times RTMP deletes a route because it was aged out of the table. This can help to detect routing problems.

`rtmpRoutingTblOvflws`
The number of times RTMP attempted to add a route to the RTMP table but failed due to lack of space.

APPLETALK ZONE INFORMATION PROTOCOL (ZIP) STATISTICS

You can display this subgroup of AppleTalk statistics by issuing the ***`atalk stats zip`*** console command.

`zipInZipQueries`
The number of ZIP Queries received by this system.

`zipInZipReplies`
The number of ZIP Replies received by this system.

`zipInZipExtReplies`
The number of ZIP Extended Replies received by this system.

`zip ZoneConflctErrors`
The number of times a conflict has been detected between this entity's zone information and another system's zone information.

`zipInObsoletes`
The number of ZIP Takedown or ZIP Bringup packets received by this system. Note that as the ZIP Takedown and ZIP Bringup packets have been obsoleted, the receipt of one of these packets indicates that a node sent it in error.

APPLETALK NAME BINDING PROTOCOL (NBP) STATISTICS

You can display this subgroup of AppleTalk statistics by issuing the *`atalk stats nbp`* console command.

`nbpInLookUpRequests`
The number of NBP LookUp Requests received.

`nbpInLookUpReplies`
The number of NBP LookUp Replies received.

`nbpInBroadcastReqs`
The number of NBP Broadcast Requests received.

`nbpInforwardRequests`
The number of NBP Broadcast Requests received.

`nbpOutLookUpReplies`
The number of NBP LookUp Replies sent.

`nbpRegistrationFails`
The number of times this node experienced a failure in attempting to register an NBP system.

`nbpInErrors`
The number of NBP packets received by this system that were rejected for any error.

APPLETALK TRANSACTION PROTOCOL (ATP) STATISTICS

You can display this subgroup of AppleTalk statistics by issuing the *`atalk stats atp`* console command.

`atpInPkts`
The number of ATP packets received by this entity.

`atpTRequestRextmis`
The number of times that a timeout occurred and a Transaction Request packet needed to be retransmitted by this host.

`atpReleaseTmExpCnts`
The number of times the release timer expired, as a result of which a Request Control Block had to be deleted.

`atpRetryCntExceeds`
The number of times the retry count was exceeded, and an error was returned to the client of ATP.

APPLETALK PORT STATISTICS

You can display the AppleTalk port statistics by issuing the *`atalk port stats`* console command.

`portInPackets`
The number of AppleTalk packets received on this port by this system.

`portOutPackets`
The number of AppleTalk packets sent out on this port by this system.

`zipInGetNetInfos`
The number of ZIP GetNetInfo packets received on this port by this system.

`zipOutGetNetInfos`
The number of ZIP GetNetInfo packets sent out this port by this system.

`zipInGetNetInfoReplies`
The number of ZIP GetNetInfo Reply packets received on this port by this system.

`zipOutGetNetInfoReplies`
The number of ZIP GetNetInfo Reply packets sent out this port by this system.

`zipZoneInInvalids`
The number of times this system has received a ZIP GetNetInfo Reply with the zone invalid bit set because the corresponding GetNetInfo Request had an invalid zone name.

`zipZoneOutInvalids`
The number of times this system has sent a ZIP GetNetInfo Reply with the zone invalid bit set in response to a GetNetInfo Request with an invalid zone name.

`zipAddressInvalids`
The number of times this system had to broadcast a ZIP GetNetInfo Reply because the GetNetInfo Request had an invalid address.

`zipInErrors`
The number of ZIP packets received by this system that were rejected for any error.

BRIDGE STATISTICS

The system collects bridge statistics for each LAN port and for WAN connections. These bridge statistics include information on the number of frames received, forwarded, discarded or transmitted. If the system is configured for two LAN ports, there is a line of counters for each LAN port. However, the WAN counters are totaled for all WAN ports.

Display bridge statistics by issuing the *br stats* command at the administration console:

`Received`
Number of frames received from a LAN port or WAN connection.

`Forwarded`
Number of frames received from LAN port 1 or LAN port 2 or all WAN ports and processed for transmission to the proper networks. Discarded frames are not forwarded for transmission.

`Discarded`
Number frames received and then discarded (i.e., not forwarded to another LAN port or WAN connection).

`Transmit`
Number of frames sent out through LAN port 1 or LAN port 2 or all WAN ports to connected networks.

Note: *Forward* refers to the passing of a *received* frame from one port to another within the CyberSWITCH. A frame can be received on any port (LAN or WAN) and forwarded to any other port, unless it is *discarded*. A forwarded frame is one which is not deliberately discarded (for example, via filters) by the CyberSWITCH. Once the frame gets to the new port, it is usually *transmitted*. However, it may not be transmitted, such as when a packet is forwarded to a WAN port, but no connection is up on that port.

CALL DETAIL RECORDING STATISTICS

You can access these statistics by issuing the *cdr stats* command.

`OutOfBuffer`
The number of times a buffer was unavailable to send a CDR report record. In this case, the intended record is discarded. The OutOfBuffer counter reflects the number of CDR records that have been discarded.

`Connects`
This counter reflects the number of connect events that have occurred since the system was loaded. This is an unsigned long integer; it will wrap after 0FFFFFFFF hex or 4,294,967,295 decimal.

`Disconnects`
This counter reflects the number of disconnect events that have occurred since the system was loaded. This is an unsigned long integer; it will wrap after 0FFFFFFFF hex or 4,294,967,295 decimal.

`Rejects`
This counter reflects the number of reject events that have occurred since the system was loaded. This is an unsigned long integer; it will wrap after 0FFFFFFFF hex or 4,294,967,295 decimal.

COMPRESSION STATISTICS

The system collects the following compression statistics for each active compression connection. These statistics can be displayed by issuing the *cmp stats* or the *cmp stats <device name>* command at the administration console. The *cmp stats* command will display the compression statistics for all active connections. The *cmp stats <device name>* command will display the compression statistics for the specified device. Note that the device name is case sensitive.

Note: When using PPP, it is possible that CCP can open with no agreed upon compression algorithm in one or both directions. In such cases, the connection is considered to be running with compression, and will consequently be picked up by the CMP command. However, the ratios and counters for the direction(s) without an actual compression algorithm negotiated will not indicate any effective compression or decompression.

COMPRESSION RELATED STATISTICS

`cmp ratio`
The number of uncompressed bytes divided by the number of compressed bytes.

`uncmp Kbytes`
The total number of uncompressed kilobytes received.

`cmp Kbytes`
The total number of compressed kilobytes sent.

`total cmp reset count`
The total number of compression resets (peer and System sent resets).

`peer sent resets`
The number of compression resets sent from peer devices.

`system sent resets`
The number of decompression resets sent from the System.

`dropped pkts`
The number of dropped packets that could not be queued.

DECOMPRESSION RELATED STATISTICS

`dmp ratio`
The number of decompressed bytes divided by the number of compressed bytes.

`dmp Kbytes`
The total number of decompressed kilobytes sent.

`cmp Kbytes`
The total number of compressed kilobytes sent.

`total dmp reset count`
The total number of decompressed resets (peer and System sent resets).

`peer sent resets`
The number of decompression resets sent from peer devices.

`system sent resets`
The number of decompression resets sent from the System.

`dropped pkts`
The number of dropped packets that could not be queued.

`fcs errors`
The number of frame checksum errors.

DHCP STATISTICS

Access DHCP statistics by using the ***`dhcp stats`*** command. The DHCP statistics are grouped into *Common DHCP statistics* (relevant to both DHCP Relay Agent and DHCP Proxy Client), *DHCP Relay Agent statistics* and *DHCP Proxy Agent statistics*.

COMMON DHCP STATISTICS

`Msgs rcvd on BOOTPS port`
Total number of UDP datagrams received on the BOOTPS UDP port. These datagrams have not been through the initial DHCP packet consistency checks yet. If packets pass these checks, they will be dispatched to either the DHCP Relay Agent or the DHCP Proxy Client.

`Msgs rcvd on BOOTPC port`
Total number of UDP datagrams received on the BOOTPC UDP port. These datagrams have not been through the initial DHCP packet consistency checks yet. If packets pass these checks, they will be dispatched to the DHCP Proxy Client.

`BOOTPS msgs sent to Relay`
Number of datagrams received on the BOOTPS port which passed the initial consistency checks, and were delivered to the DHCP Relay Agent.

`BOOTPS msgs sent to Proxy`
Number of datagrams received on the BOOTPS port which passed the initial consistency checks, and were delivered to the DHCP Proxy Client.

`BOOTPS msgs discarded`
Number of datagrams received on the BOOTPS port which were discarded without being dispatched to either the DHCP Proxy Client or the DHCP Relay Agent. Normally, any datagrams the Proxy Client does not want are forwarded to the Relay Agent. But if the Relay Agent is not enabled, these datagrams are discarded.

`DHCP/BOOTP msg too small`
Stat incremented whenever a DHCP/BOOTP message is received with a total length less than the minimum BOOTP header length. Messages that are too small are discarded.

`DHCP/BOOTP invalid'op'`
Stat incremented whenever a DHCP/BOOTP message is received with an'op' field that is not equal to either BOOTREQUEST or BOOTREPLY. These messages are discarded.

DHCP RELAY AGENT STATISTICS

`BOOTREQUEST msgs rcvd`
Incremented whenever the system identifies a UDP datagram as a DHCP/BOOTP BOOTREQUEST message. This datagram has passed the initial consistency checks.

`BOOTREQUEST msgs rlyd`
Incremented whenever the system has successfully "relayed" a BOOTREQUEST message to a configured destination (i.e., another Relay Agent, or a DHCP/BOOTP server).

`BOOTREQUEST no dests cfg`
Number of DHCP/BOOTP BOOTREQUEST messages received by the DHCP Relay Agent that were discarded due to the fact that there weren't any relay destination addresses configured.

`BOOTREQUEST over max hops`
Incremented whenever the DHCP Relay Agent has received a DHCP/BOOTP BOOTREQUEST message with a 'hops' field that has exceeded the maximum allowable value. These messages are discarded.

`BOOTREQUEST no giaddr I/F`
Number of DHCP/BOOTP BOOTREQUEST messages received by the DHCP Relay Agent with 'giaddr' fields of '0.0.0.0' that were discarded due to the fact that they were received over unnumbered interfaces. It will not be possible to return a reply to the client, since we have not determined on which network interface the client is located.

`BOOTREQUEST bad rly dest`
Number of DHCP/BOOTP BOOTREQUEST messages received by the DHCP Relay Agent that were discarded due to the fact that the Relay Agent must not rebroadcast messages on the same network interface on which they were received.

`BOOTREQUEST msg too big`
Number of times that the DHCP Relay Agent aborted sending a BOOTREQUEST message due to the fact that the message was too big to fit into a buffer allocated from the Relay Agent's transmit buffer pool.

`BOOTREQUEST no buffer`
Incremented whenever the DHCP Relay Agent cannot successfully get a buffer from the Relay Agent's transmit buffer pool when trying to relay BOOTREQUEST messages to multiple destinations.

`BOOTREQUEST xmit fail`
Number of UDP subsystem errors returned to the DHCP Relay Agent while it was trying to send BOOTREQUEST messages to configured destinations.

`BOOTREPLY msgs rcvd`
Incremented whenever the system identifies a UDP datagram as a DHCP/BOOTP BOOTREPLY message. This datagram has passed the initial consistency checks.

`BOOTREPLY msgs rlyd`
Number of BOOTREPLY messages that were successfully relayed to DHCP/BOOTP clients.

`BOOTREPLY bad 'giaddr':`
Number of DHCP/BOOTP BOOTREPLY messages that were discarded by the DHCP Relay Agent because the 'giaddr' (gateway IP address) field could not be mapped to one of the system's IP network interfaces.

`BOOTREPLY arp_add0 fail`
Number of times that the DHCP/BOOTP Relay Agent failed to add a client's IP address/hardware address pair to the ARP table. When this occurs, an attempt is still made to send the BOOTREPLY to the client.

`BOOTREPLY xmit fail`
Number of UDP subsystem errors returned to the DHCP Relay Agent while it was trying to send BOOTREPLY messages to DHCP clients.

DHCP Proxy Client Statistics

`DHCPDISCOVERS sent`
Incremented whenever the DHCP Proxy Client has successfully broadcasted a DHCPDISCOVER message.

`DHCPDISCOVERS xmit fail`
Incremented whenever an unsuccessful result is returned from UDP, when the DHCP Proxy Client was trying to broadcast a DHCPDISCOVER message.

`DHCPREQUESTS sent`
Incremented whenever the DHCP Proxy Client has successfully sent a DHCPREQUEST message.

`DHCPREQUEST xmit fail`
Incremented whenever an unsuccessful result is returned from UDP, when the DHCP Proxy Client was trying to send a DHCPREQUEST message.

`DHCPRELEASEs sent`
Incremented whenever the DHCP Proxy Client has successfully sent a DHCPRELEASE message.

`DHCPRELEASE xmit fail`
Incremented whenever an unsuccessful result is returned from UDP, when the DHCP Proxy Client was trying to send a DHCPRELEASE message.

`DHCPDECLINE sent`
Incremented whenever the DHCP Proxy Client has successfully sent a DHCPDECLINE message.

`DHCPDECLINE xmit fail`
Incremented whenever an unsuccessful result is returned from UDP, when the DHCP Proxy Client was trying to send a DHCDECLINE message.

`DHCPOFFERSs recd`
Incremented whenever the DHCP Proxy Client has received a DHCPOFFER message from a DHCP server.

`DHCPACKs rcvd`
Incremented whenever the DHCP Proxy Client has received a DHCPACK message from a DHCP server.

`DHCPNAKs rcvd`
Incremented whenever the DHCP Proxy Client has received a DHCPNAK message from a DHCP server.

`Invalid DHCP pkts rcvd`
Incremented whenever the DHCP Proxy Client encounters a DHCP message that is invalid due to either of the following:

- the 'op' field is not equal to BOOTREPLY
- the DHCP 'special field' is not found at the beginning of the options field

When this occurs, the packet is silently discarded.

`Invalid XID rcvd`
Incremented whenever the DHCP Proxy Client manager receives a DHCP message with a transaction ID that was not reserved by any of the underlying DHCP client invocations. When this occurs, the packet is silently discarded.

`No xmt buffer available`
Incremented whenever the DHCP Proxy Client cannot successfully get a buffer from the Proxy Client's transmit buffer pool. This can happen whenever we are trying to send BOOTREQUEST messages to a DHCP server.

DIGITAL MODEM STATISTICS

If you are using a Digital Modem, you can access the following statistics by using the *`modem stats`* command:

`pkts rcvd`
Total number of packets received over the modem connection.

`pkts xmit`
Total number of packets transmitted over the modem connection.

`fcs errors`
Total number of HDLC frames discarded because of Frame Checksum (FCS) errors.

FRAME RELAY STATISTICS

You can access these statistics by issuing the *`fr stats`* console command. The statistics displayed will be associated with the currently selected Access and DLCI.

ACCESS RELATED STATISTICS

`Access State`
The condition of the Frame Relay Access. Possible values are TERMINATED, INIT, UP, and DOWN. The definitions for the possible values are as follows:

`TERMINATED`
The access state entered when the access is dynamically removed.

INIT
The access state entered when the access is first initialized. The access has entered the LMI dialogue phase, but has not yet received an appropriate LMI STATUS message response.

UP
The access state entered when the access either has no LMI, or the LMI message exchange is confirmed.

DOWN
The access state entered when the access has been lost due to layer 1 loss, or after no response has been received on the LMI link.

Line Ready Count
The number of times the physical link underlying the Frame Relay Access has become "ready" for use.

Line Not Ready Count
The number of times the physical link underlying the Frame Relay Access has become unusable.

Frames Received
The total number of frames received on the Frame Relay Access. This is the sum of the number of frames received on each PVC associated with this access.

Frames Sent
This item refers to the total number of frames sent on the Frame Relay Access. This is the sum of the number of frames sent on each PVC associated with this access.

Bytes Received
The total number of bytes received on the Frame Relay Access. This is the sum of the number of bytes received on each PVC associated with this access.

Bytes Sent
The total number of bytes sent on the Frame Relay Access. This is the sum of the number of bytes sent on each PVC associated with this access.

Reset Rx Seq
The number of times the receive sequence variable had to be reset. This event occurs when a receive sequence number of '0' is received from the network.

Reset Tx Seq
The number of times the transmit sequence variable had to be reset. This event occurs when a transmit sequence number of '0' is received from the network.

Lost Rx Seq
The number of times a receive frame was lost. This event is indicated by a break in the receive sequence numbers of received frames (i.e., the receive sequence number of a particular receive frame did not compare with the software's expected receive sequence number).

Lost Tx Seq
The number of times a transmit frame was lost. This event is indicated by a break in the transmit sequence numbers of received frames (i.e., the transmit sequence number of a particular receive frame did not compare with the software's expected transmit sequence number).

`# Lost Rx Frame`
Related to the "# Lost Rx Seq" counter in that it represents the number of actual lost frames, not just the number of times a frame (or frames) was lost.

`# Invalid Frame Size`
The number of times a frame is discarded because it exceeded the maximum frame size supported by the frame relay network.

`# Timed Lost Rx Frame`
Not currently supported.

`# No Control Block`
Not currently supported.

`# NEW & Existing PVC`
The number of times a NEW PVC was indicated by a LMI STATUS message—but the frame relay software believed the PVC already existed.

`# PVC Not Configured`
The number of times a frame was received containing an unknown DLCI value, and hence, an unconfigured PVC.

`# No NEW Bit`
Not currently supported.

`# Not Full ENQUIRY`
The number of times a `STATUS` message was received containing a `LINK INTEGRITY VERIFICATION ONLY` report type, when in fact a `FULL REPORT` was expected.

`# Errored Full ENQUIRY`
The number of times an errored `STATUS` message was received of type `FULL REPORT`.

`# Delete Absent PVC`
Not currently supported.

`# Errored LMI Header`
The number of LMI frames received in which the LMI encapsulation header was errored.

PVC RELATED STATISTICS

`PVC State`
The condition of the Frame Relay Permanent Virtual Circuit. Possible values are: `TERMINATED, INIT, NOT READY,` and `NETWORK OUTAGE`. The definitions for the possible values are as follows:

`TERMINATED`
The PVC state entered when the PVC has been dynamically removed.

`INIT`
The PVC state entered when the PVC is ready for use.

NOT READY
The PVC state entered when the PVC has been marked unavailable by the network via a STATUS message, an alarm condition, or failure of the LMI link.

NETWORK OUTAGE
The PVC state entered when the PVC has been marked unavailable. This follows the receipt of a CLLM message indicating a network failure has occurred.

PVC activations
The number of times the PVC has been marked available for use, or "up".

PVC deactivations
The number of times the PVC has been marked unavailable for use, or "down".

Frames received
The total number of frames received on the PVC.

Bytes received
The total number of bytes received on the PVC.

Frames sent
The total number of frames sent on the PVC.

Bytes sent
The total number of bytes sent on the PVC.

Flow Control Events
The number of times the PVC was congested due to busy transmit hardware.

No registered device
The number of times a frame is received on a PVC which is configured, but not associated with any Frame Relay Service Device.

Current receive rate
The currently enforced receive data rate, taking into account congestion.

Current transmit rate
The currently enforced transmit data rate, taking into account congestion.

LAN STATISTICS

You can access LAN statistics by issuing the *lan stats* console command.

pkts rcvd
The total number of packets received on the LAN port.

rcv overruns
The number of frames known to be lost because the local system bus was not available. If the traffic problem persists for more than one frame, the frames that follow the first are also lost; however, because there is no lost frame indicator they are not counted.

`crc errors`
The number of aligned frames discarded because of a CRC error.

`align errors`
The number of frames that are both misaligned and contain a CRC error.

`resource errors`
The number of good frames discarded because there were no resources available.

`pkts xmit`
The number of packets transmitted on the LAN port.

`xmit errors`
The number of packets transmitted with errors on the LAN port.

IP STATISTICS

You can access IP statistics by using the ***`ip stats`*** console command. These statistics are parts of the IP Group and the ICMP Group MIB variables that are defined in RFC-1213:MIB-II.

IP GROUP STATISTICS

`ipForwarding`
The indication of whether the system is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, this CyberSWITCH. IP gateways forward datagrams, IP hosts do not (except those source-routed via the host).

`ipDefaultTTL`
The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this system, whenever a TTL value is not supplied by the transport layer protocol.

`ipInReceives`
The total number of input datagrams received from interfaces, including those received in error.

`ipInHdrErrors`
The number of input datagrams discarded due to errors in their IP headers. Possible errors include bad checksums, version number mismatches, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.

`ipInAddrErrors`
The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this system. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For systems that are not IP Gateways, and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.

`ipForwDatagrams`
The number of input datagrams for which this system was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In systems that do not act as IP Gateways, this counter will include only those packets that were Source-Routed via this system, and the Source-Route option processing was successful.

`ipInUnknownProtos`
The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

`ipInDiscards`
The number of input IP datagrams for which no problems were encountered that would prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.

`ipInDelivers`
The total number of input datagrams successfully delivered to IP device-protocols (including ICMP).

`ipOutRequests`
The total number of IP datagrams which local IP device-protocols (including ICMP) supplied to IP in requests for transmission.

`ipOutDiscards`
The number of output IP datagrams for which no problem was encountered that would prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.

`ipOutNoRoutes`
The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams that meet this "no-route" criterion. Note that this includes any datagrams that a host cannot route because all of its default gateways are down.

`ipReasmTimeout`
The maximum number of seconds that received fragments are held while they are awaiting reassembly at this system.

`ipReasmReqds`
The number of IP fragments received which needed to be reassembled at this system.

`ipReasmOKs`
The number of IP datagrams successfully reassembled.

`ipReasmFails`
The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.

`ipFragOKs`
The number of IP datagrams that have been successfully fragmented at this system.

`ipFragFails`
The number of IP datagrams that have been discarded because they needed to be fragmented at this system but could not be, for example, because their "Don't Fragment" flag was set.

`ipFragCreates`
The number of IP datagram fragments that have been generated as a result of fragmentation at this system.

ICMP GROUP STATISTICS

`icmpInMsgs`
The total number of ICMP messages that the system received. Note that this counter includes all those counted by icmpInErrors.

`icmpInErrors`
The number of ICMP messages that the system received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).

`icmpInDestUnreachs`
The number of ICMP Destination Unreachable messages received.

`icmpInTimeExcds`
The number of ICMP Time Exceeded messages received.

`icmpInParmProbs`
The number of ICMP Parameter Problem messages received.

`icmpInSrcQuenchs`
The number of ICMP Source Quench messages received.

`icmpInRedirects`
The number of ICMP Redirect messages received.

`icmpInEchos`
The number of ICMP Echo (request) messages received.

`icmpInEchoReps`
The number of ICMP Echo Reply messages received.

`icmpInTimestamps`
The number of ICMP Timestamp (request) messages received.

`icmpInTimestampReps`
The number of ICMP Timestamp Reply messages received.

`icmpInAddrMasks`
The number of ICMP Address Mask Request messages received.

`icmpInAddrMaskReps`
The number of ICMP Address Mask Reply messages received.

`icmpOutMsgs`
The total number of ICMP messages that this system attempted to send. Note that this counter includes all those counted by icmpOutErrors.

`icmpOutErrors`
The number of ICMP messages that this system did not send due to problems discovered within ICMP, such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no error types that contribute to this counter's value.

`icmpOutDestUnreachs`
The number of ICMP Destination Unreachable messages sent.

`icmpOutTimeExcds`
The number of ICMP Time Exceeded messages sent.

`icmpOutParmProbs`
The number of ICMP Parameter Problem messages sent.

`icmpOutSrcQuenchs`
The number of ICMP Source Quench messages sent.

`icmpOutRedirects`
The number of ICMP Redirect messages sent. For a host, this will always be zero, since hosts do not send redirects.

`icmpOutEchos`
The number of ICMP Echo (request) messages sent.

`icmpOutEchoReps`
The number of ICMP Echo Reply messages sent.

`icmpOutTimestamps`
The number of ICMP Timestamp (request) messages sent.

`icmpOutTimestampReps`
The number of ICMP Timestamp Reply messages sent.

`icmpOutAddrMasks`
The number of ICMP Address Mask Request messages sent.

`icmpOutAddrMaskReps`
The number of ICMP Address Mask Reply messages sent.

IPX STATISTICS

You can access the following types of IPX statistics: general, RIP and triggered RIP, SAP and triggered SAP and IPX spoofing. The sections below provide information for each category.

IPX GENERAL STATISTICS

You can access IPX general statistics by using the *`ipx stats`* console command. IPX general statistics include basic and advanced system table statistics.

IPX BASIC SYSTEM TABLE STATISTICS

`ipxBasicSysExistState`
The validity of this entry in the IPX system table. Setting this field to off indicates that this entry may be deleted from the system table at the IPX implementation's discretion.

`ipxBasicSysNetNumber`
The network number portion of the IPX address of this system.

`ipxBasicSysName`
The readable name for this system.

`ipxBasicSysInReceives`
The total number of IPX packets received, including those received in error.

`ipxBasicSysInHdrErrors`
The number of IPX packets discarded due to errors in their headers, including any IPX packet with a size less than the minimum of 30 bytes.

`ipxBasicSysInUnknownSockets`
The number of IPX packets discarded because the destination socket was not open.

`ipxBasicSysInDiscards`
The number of IPX packets received but discarded due to reasons other than those accounted for by ipxBasicSysInHdrErrors, ipxBasicSysInUnknownSockets, ipxAdvSysInDiscards, and ipxAdvSysInCompressDiscards.

`ipxBasicSysInBadChecksums`
The number of IPX packets received with incorrect checksums.

`ipxBasicSysInDelivers`
The total number of IPX packets delivered locally including packets from local applications.

`ipxBasicSysNoRoutes`
The number of times no route to a destination was found.

`ipxBasicSysOutRequests`
The number of IPX packets supplied locally for transmission, not including any packets counted in ipxAdvForwPackets.

`ipxBasicSysOutMalformedRequests`
The number of IPX packets supplied locally that contained errors in their structure.

`ipxBasicSysOutDiscards`
The number of outgoing IPX packets discarded due to reasons other than those accounted for in ipxBasicSysOutMalformedRequests, ipxAdvSysOutFiltered and ipxAdvSysOutCompressDiscards.

`ipxBasicSysOutPackets`
The total number of IPX packets transmitted.

`ipxBasicSysConfigSockets`
The configured maximum number of IPX sockets that may be open at one time.

`ipxBasicSysOpenSocketFails`
The number of IPX socket open calls which failed.

IPX ADVANCED SYSTEM TABLE STATISTICS

`ipxAdvSysMaxPathSplits`
The maximum number of paths with equal routing metric value which this instance of the IPX may split between when forwarding packets.

`ipxAdvSysMaxHops`
The maximum number of hops a packet may take.

`ipxAdvSysInTooManyHops`
The number of IPX packets discarded due to exceeding the maximum hop count.

`ipxAdvSysInFiltered`
The number of incoming IPX packets discarded due to filtering.

`ipxAdvSysInCompressDiscards`
The number of incoming IPX packets discarded due to decompression errors.

`ipxAdvSysNETBIOSPackets`
The number of NETBIOS packets received.

`ipxAdvSysForwPackets`
The number of IPX packets forwarded.

`ipxAdvSysOutFiltered`
The number of outgoing IPX packets discarded due to filtering.

`ipxAdvSysOutCompressDiscards`
The number of outgoing IPX packets discarded due to compression errors.

`ipxAdvSysCircCount`
The number of circuits known to this instance of IPX.

`ipxAdvSysDestCount`
The number of currently reachable destinations known to this instance of IPX.

`ipxAdvSysServCount`
The number of services known to this instance of IPX.

IPX RIP STATISTICS

You can access IPX RIP statistics by using the *`ipx rip stats`* console command.

`ripInstance`
With the CyberSWITCH, the value of this statistic is always 1. With other products, this statistic is useful. Currently, it is not useful for the CyberSWITCH.

`ripIncorrectPackets`
The number of times incorrect RIP packets were received.

`ripState`
Represents the status of the IPX RIP feature: 1 = disabled, 2 = enabled.

IPX TRIGGERED RIP STATISTICS

You can access IPX triggered RIP statistics by using the ***`ipx trigrip stats`*** command.

trigRipUpdateRequestsSent
Number of triggered RIP update requests sent.

trigRipUpdateRequestsRcvd
Number of triggered RIP update requests received.

trigRipUpdateResponsesSent
Number of triggered RIP update responses sent.

trigRipUpdateResponsesRcvd
Number of triggered RIP update responses received.

trigRipUpdateAcksSent
Number of triggered RIP update acknowledgments sent.

trigRipUpdateAcksRcvd
Number of triggered RIP update acknowledgments received.

trigRipInputErrors
Number of Triggered RIP input message errors.

IPX ROUTE STATISTICS

You can access IPX Route statistics by using the ***`ipx route stats`*** console command.

`Static Routes`
Number of static routes configured on this router.

`Rip Routes`
Number of routes learned through RIP from other routers.

`Internal Routes`
Number of internal routes on this router. There is one for the internal network number, and two for each IPX network interface.

`Total Routes`
Total number of routes. Should be equal to the sum of Static, RIP and Internal Routes.

`Maximum Routes`
Maximum number of routes this router is configured to handle.

`Available Routes`
Number of routes currently available on this router.

`High Water Mark`
Peak number of routes this router has used.

IPX SAP STATISTICS

You can access IPX SAP statistics by using the *`ipx sap stats`* console command.

`sapInstance`
With the CyberSWITCH, the value of this statistic is always 1. With other products, this statistic is useful. Currently, it is not useful for the CyberSWITCH.

`sapIncorrectPackets`
The number of times incorrect SAP packets were received.

`sapState`
Represents the status of the IPX SAP feature: 1 = disabled, 2 = enabled.

IPX TRIGGERED SAP STATISTICS

You can access IPX triggered SAP statistics by using the *`ipx trigsap stats`* command.

`trigSapUpdateRequestsSent`
Number of triggered SAP update requests sent.

`trigSapUpdateRequestsRcvd`
Number of triggered SAP update requests received.

`trigSapUpdateResponsesSent`
Number of triggered SAP update responses sent.

`trigSapUpdateResponsesRcvd`
Number of triggered SAP update responses received.

`trigSapUpdateAcksSent`
Number of triggered SAP update acknowledgments sent.

`trigSapUpdateAcksRcvd`
Number of triggered SAP update acknowledgments received.

`trigSapInputErrors`
Number of Triggered SAP input message errors.

IPX SERVICE STATISTICS

You can access IPX Service statistics by using the *ipx service stats* console command.

`Static Services`
Number of static services configured on this router.

`Sap Services`
Number of services learned through SAP from other routers.

`Total Services`
Total number of services. Should be equal to the sum of Static and SAP services.

`Maximum Services`
Maximum number of services this router is configured to handle.

`Available Services`
Number of services currently available on this router.

`High Water Mark`
Peak number of services this router has used.

RIP STATISTICS

You can access RIP statistics by using the *ip rip stats* console command. Global RIP statistics and statistics for each configured RIP interface are included.

RIP GLOBAL STATISTICS

`GlobalRouteChanges`
The number of route changes made to the IP route database by RIP. This does not include the refresh of a route's age.

`GlobalQueries`
The number of responses sent to RIP queries from other systems.

RIP INTERFACE STATISTICS

The following set of RIP interface statistics are displayed for each configured RIP interface.

`IfStatAddress`
The IP address of this system on the indicated RIP interface. For unnumbered interfaces, the value 0.0.0.N, where the last signification 24 bits (N) is the index for the IP interface in network byte order.

`IfStatRcvBadPackets`
The number of RIP response packets received by the RIP process which were subsequently discarded for any reason. Example reasons include: a version 0 packet, or an unknown command type.

`IfStatRcvBadRoutes`
The number of routes, in valid RIP packets, which were ignored for any reason. Example reasons include: an unknown address family, or an invalid metric.

`IfStatRcvRequests`
The number of RIP messages with 'request' command code received on this interface.

`IfStatRcvResponses`
The number of RIP messages with 'response' command code received on this interface.

`IfStatSentRequests`
The number of RIP messages with 'request' command code sent on this interface.

`IfStatSentResponses`
The number of RIP messages with 'response' command code sent on this interface.

`IfStatSentUpdates`
The number of triggered RIP updates actually sent on this interface. This explicitly does NOT include full updates sent containing new information.

SERIAL INTERFACE STATISTICS

Access these statistics by using the *ser <#> stats* command:

`frames sent`
Number of frames successfully sent over a serial interface line.

`frames received`
Number of frames successfully received over a serial interface line.

`transmit errors`
Number of errors that occurred while sending a frame over a serial interface line.

`receive errors`
Number of errors that occurred while receiving a frame from a serial interface line.

SNMP STATISTICS

If the SNMP Agent is enabled, you can access SNMP statistics by using the ***`snmp stats`*** command. Each of the following statistics are counters that refer to an MIB-2 SNMP group object.

`snmpInPkts`
The total number of messages delivered to the SNMP Agent from the transport service.

`snmpOutPkts`
The total number of SNMP messages that were passed from the SNMP Agent to the transport service.

`snmpInBadVersions`
The total number of SNMP messages that were delivered to the SNMP Agent and were for an unsupported SNMP version.

`snmpInBadCommunityNames`
The total number of SNMP messages delivered to the SNMP Agent that used an SNMP community name not known to said system.

`snmpInBadCommunityUses`
The total number of SNMP messages delivered to the SNMP Agent that represented an SNMP operation that was not allowed by the SNMP community named in the message.

`snmpInASNParseErrs`
The total number of ASN.1 or BER errors encountered by the SNMP Agent when decoding received SNMP messages.

`snmpInTooBigs`
The total number of SNMP PDUs that were delivered to the SNMP Agent and for which the value of the error-status field is “tooBig”.

`snmpInNoSuchNames`
The total number of SNMP PDUs that were delivered to the SNMP Agent and for which the value of the error-status field is “noSuchName”.

`snmpInBadValues`
The total number of SNMP PDUs that were delivered to the SNMP Agent and for which the value of the error-status field is “badValue”.

`snmpInReadOnlys`
The total number of valid SNMP PDUs that were delivered to the SNMP Agent and for which the value of the error-status field is “readOnly”. It should be noted that it is a protocol error to generate an SNMP PDU that contains the value “readOnly” in the error-status field, as such this object is provided as a means of detecting incorrect implementations of the SNMP.

`snmpInGenErrs`
The total number of SNMP PDUs that were delivered to the SNMP Agent and for which the value of the error-status field is “genErr”.

`snmpInTotalReqVars`
The total number of MIB objects that have been retrieved successfully by the SNMP Agent as the result of receiving valid SNMP Get-Request and Get-Next PDUs.

`snmpInTotalSetVars`
The total number of MIB objects that have been altered successfully by the SNMP Agent as the result of receiving valid SNMP Set-Request PDUs.

`snmpInGetRequests`
The total number of SNMP Get-Request PDUs that have been accepted and processed by the SNMP Agent.

`snmpInGetNexts`
The total number of SNMP Get-Next PDUs that have been accepted and processed by the SNMP Agent.

`snmpInSetRequests`
The total number of SNMP Set-Request PDUs that have been accepted and processed by the SNMP Agent.

`snmpInGetResponses`
The total number of SNMP Get-Response PDUs that have been accepted and processed by the SNMP Agent.

`snmpInTraps`
The total number of SNMP Trap PDUs that have been accepted and processed by the SNMP Agent.

`snmpOutTooBigs`
The total number of SNMP PDUs that were generated by the SNMP Agent and for which the value of the error-status field is "tooBig".

`snmpOutNoSuchNames`
The total number of SNMP PDUs that were generated by the SNMP Agent and for which the value of the error-status is "noSuchName".

`snmpOutBadValues`
The total number of SNMP PDUs that were generated by the SNMP Agent and for which the value of the error-status field is "badValue".

`snmpOutGenErrs`
The total number of SNMP PDUs that were generated by the SNMP Agent and for which the value of the error-status field is "genErr".

`snmpOutGetRequests`
The total number of SNMP Get-Request PDUs that have been generated by the SNMP Agent.

`snmpOutGetNexts`
The total number of SNMP Get-Next PDUs that have been generated by the SNMP Agent.

`snmpOutSetRequests`
The total number of SNMP Set-Request PDUs that have been generated by the SNMP Agent.

`snmpOutGetResponses`
The total number of SNMP Get-Response PDUs that have been generated by the SNMP Agent.

`snmpOutTraps`
The total number of SNMP Trap PDUs that have been generated by the SNMP Agent.

`snmpEnableAuthenTraps`
Indicates whether the SNMP agent process is permitted to generate authentication-failure traps. The value of this object overrides any configuration information. For example, it provides a means whereby all authentication-failure traps may be disabled.

TCP STATISTICS

You can access these statistics by issuing the *tcp stats* console command.

`tcpRtoAlgorithm`
The algorithm used to determine the timeout value used for retransmitting unacknowledged octets. This value is always equal to 4 for the Van Jacobson's algorithm.

`tcpRtoMin`
The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds.

`tcpRtoMax`
The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds.

`tcpMaxConn`
The limit on the total number of TCP connections the system can support.

`tcpActiveOpens`
The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.

`tcpPassiveOpens`
The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.

`tcpAttemptFails`
The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.

`tcpEstabResets`
The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.

`tcpCurrEstab`
The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT. This counter is not currently kept up to date.

`tcpInSegs`
The total number of segments received, including those received in error. This count includes segments received on currently established connections.

`tcpOutSegs`
The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.

`tcpRetransSegs`
The total number of segments retransmitted (the number of tcp segments transmitted containing one or more previously transmitted octets).

`tcpInErrs`
The total number of segments received in error (for example, bad TCP checksums).

`tcpOutRsts`
The number of TCP segments sent containing the RST flag.

TFTP STATISTICS

You can access these statistics by issuing the *`tftp stats`* console command.

STATISTICS FOR SERVER OR REMOTE INITIATED TFTP ACTIVITY

`Successful file puts`
Displays the count of the successful puts from the remote hosts.
(Remote host uploaded a file to local system.)

`Successful file gets`
Displays the count of the successful gets from the remote hosts.
(Remote host downloaded a file from the local system.)

`Failed file puts`
Displays the count of failed puts.
(Remote host failed to upload a file to the local system.)

`Failed file gets`
Displays the count of failed gets.
(Remote host failed to download a file from the local system.)

`Total bytes put`
Displays the total number of bytes successfully put.
(Number of bytes uploaded to the local system by remote hosts.)

`Total bytes get`
Displays the total number of bytes successfully gotten.
(Number of bytes downloaded from the local system by remote hosts.)

STATISTICS FOR LOCAL OR CLIENT INITIATED TFTP ACTIVITY

`Successful file puts`
Displays the count of successful puts from the local system.
(Files uploaded from the local system to remote hosts.)

`Successful file gets`
Displays the count of successful gets to the local system.
(Files downloaded from remote hosts to the local system.)

`Failed file puts`
Displays the count of failed puts.
(Local system failed to upload a file to a remote host.)

`Failed file gets`
Displays the count of failed gets.
(Local system failed to download a file from a remote host.)

`Total bytes put`
Displays the total number of bytes successfully put.
(Number of bytes uploaded from the local system to remote hosts.)

`Total bytes get`
Displays the total number of bytes successfully gotten.
(Number of bytes downloaded from remote hosts to the local system.)

STATISTICS FOR ALL TFTP ACTIVITY

`Read Requests Sent`
Displays the total number of Read Requests sent.

`Read Requests Received`
Displays the total number of Read Requests received.

`Write Requests Sent`
Displays the total number of Write Requests sent.

`Write Requests Received`
Displays the total number of Write Requests received.

`Data Packets Sent`
Displays the total number of Data Packets sent.

`Data Packets Received`
Displays the total number of Data Packets received.

`Error Packets Sent`
Displays the total number of Error Packets sent.

`Error Packets Received`
Displays the total number of Error Packets received.

`ACK Packets Sent`
Displays the total number of ACK Packets sent.

`ACK Packets Received`
Displays the total number of ACK packets received.

`TFTP Sessions Opened`
Displays the total number of TFTP Sessions that have been opened.

`TFTP Sessions Closed`
Displays the total number of TFTP Sessions that have been closed.

`TFTP Sessions still open`
Displays the total number of TFTP Sessions that are still open.

UDP STATISTICS

If the IP operating mode is enabled, you can access the following UDP statistics by using the *udp stats* command:

`udpInDatagrams`
The total number of UDP datagrams delivered to UDP devices.

`udpInErrors`
The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.

`udpNoPorts`
The total number of received UDP datagrams for which there was no application at the destination port.

`udpOutDatagrams`
The total number of UDP datagrams sent from this system.

WAN FR_IETF STATISTICS

You can access FR_IETF statistics by issuing the *wan fr-ietf stats [device/ fr_accessname_dlci] [prot]* console command.

`Protocol`
The line protocol of the packets transmitted or received.

`Frames Sent`
The number of frames sent for the indicated protocol.

`Octets Sent`
The number of octets sent for the indicated protocol.

`Send Errors`
The number of transmission errors for the indicated protocol.

`Frames Received`
The number of frames received for the indicated protocol.

`Octets Received`
The number of octets received for the indicated protocol.

`Receive Errors`
The number of errored frames received for the indicated protocol.

WAN L1P STATISTICS

You can access WAN L1P statistics by issuing the *wan l1p stats display <slot #>* console command. These statistics are divided into the following groups of statistics: PRI S/T (T1/E1) interface statistics, error statistics, and layer 1 general statistics. These groups are defined below.

PRI S/T (T1/E1) INTERFACE STATISTICS

`Layer 1 Up`
The number of times layer 1 has reported itself up to the upper ISDN layers.

`Layer 1 Down`
The number of times layer 1 has reported itself down to the upper ISDN layers.

`L1 Deactivates`
The number of times the upper ISDN layers requested layer 1 to deactivate.

`Loss of Frame (RED)`
The number of times layer 1 has detected a qualified loss of frame condition; excluding AIS (alarm indication signal).

`Loss of Signal (RED)`
The number of times layer 1 has detected an all zero signal (or complete lack of signal).

`AIS (Blue)`
The number of times layer 1 has detected a qualified unframed all ones signal.

`RAI (Yellow)`
The number of times layer 1 has detected a qualified RAI (remote alarm indication) signal.

LAYER 1 PRI ERROR STATISTICS

Note: Layer 1 PRI error statistics apply to the line connected to the indicated slot.

`Bipolar Violations`
The number or times there has been either a mismatch between encoding types (B8ZS not selected) or line noise.

`ESF CRC Errors`
The number of Cyclic Redundancy Check (CRC) errors in the PRI framing format (ESF framing only).

`Framing Bit Errors`
The number of errors in the framing bits of the PRI layer 1 framing format.

`Recv Negative Slips`
The Number of PRI frames lost due to timing problems in the negative direction.

`Global Parity Errors`
The number of parity errors seen across all transmit and receive channels.

`Recv Positive Slips`
The number of PRI frames lost due to timing problems in the positive direction.

`Recv Parity Errors`
The number of receive parity errors.

`Xmit Slips`
The number of times an error has occurred in the host clock system. If the wander of the transmit route clock is too great, data transmission errors will occur.

`Xmit Parity Errors`
The number of transmit parity errors.

LAYER 1 GENERAL STATISTICS

Note: Layer 1 general statistics apply to the indicated slot.

`Interrupts`
The number of hardware interrupts received from the layer 1 hardware device.

`Forced Resynchs`
The number of times layer 1 has attempted to manually synchronize to the incoming signal.

`Unknown Events`
If this counter is ever non-zero, call Customer Support Personnel.

`Unused Events`
If this counter is ever non-zero, call Customer Support Personnel.

`Unknown Mail`
If this counter is ever non-zero, call Customer Support Personnel.

`Wrong State`
If this counter is ever non-zero, call Customer Support Personnel.

WAN STATISTICS

You can access WAN statistics by issuing the *`wan stats`* console command.

`data link up`
A counter that is incremented every time a data link comes up.

`data link down`
A counter that is incremented each time a data link goes down.

`switched call initiated`
A counter that is incremented for each attempt to make a switched call.

`switched call completed`
A counter that is incremented each time a switched call successfully completes and passes identification.

`switched call retry`
A counter that is incremented for each retry of an original switched call attempt.

`switched call not possible`
A counter that is incremented each time a switched call needs to be made to a site and it is not possible.

`connection request failure`
A counter that is incremented each time a connection is requested and no response has been received after a connection request failure period of time.

`rcv fail`
A counter that is incremented each time an incoming connection is accepted and no response has been received after a connection receive failure period of time.

`wan board recover`
A counter that is incremented each time a WAN board is restarted after it originally comes up.

`call minutes (day)`
The total call minutes that have been logged for the day.

`call minutes (month)`
The total call minutes that have been logged for the month.

`calls (day)`
The total number of calls that have been made for the day.

`calls (month)`
The total number of calls that have been made for the month.

X.25 STATISTICS

There are two sets of statistics available related to an X.25 access: statistics for the access itself, and statistics for specific Virtual Circuits (VCs) used by the X.25 access.

X.25 ACCESS RELATED STATISTICS

You can access these statistics by issuing the *`x25 stats`* console command. The statistics displayed will be associated with the currently selected Access and LCN.

`Local Address`
The X.121 address of the local DTE.

`Subnet ID`
The subnet Id of the local DTE.

Max Connections
The maximum number of active VCs allowed at any time.

Active Conn
The number of currently active VCs.

Max Conn Active
The maximum number of VCs that can be active at any time.

Conn Failed
The number of VCs that have failed.

Normal Disconnect
The number of SVC connections that terminated normally.

Abnrml Disconnect
The number of VC connections that terminated due to LAPB problems.

Packets Sent count
The number of X.25 data packets sent.

Packets Received
The number of X.25 data packets received.

Resets Sent count
The number of resets sent.

Resets Received
The number of resets received.

RR Sent count
The number of receive ready packets sent.

RR Received
The number of receive ready packets received.

RNR Sent count
The number of receive not ready packets sent.

RNR Received
The number of receive not ready packets received.

REJ Sent count
The number of remote connection requests that have been rejected.

REJ Received
The number of locally generated connection requests that have been rejected.

Restarts Sent
The number of times the X.25 network has been restarted by the local DTE.

`# Restarts Received`
The number of times the X.25 network has been restarted by a remote DTE or the network.

`# Diag Pkt Sent`
The number of diagnostic packets sent.

`# Diag Pkt Received`
The number of diagnostic packets received.

`# Bytes Sent count`
The total number of data bytes sent.

`# Bytes Received`
The total number of data bytes received.

X.25 VIRTUAL CIRCUIT (VC) RELATED STATISTICS

You can access these statistics by issuing the *`x25 vc stats`* console command. The statistics displayed will be associated with the currently selected default VC.

`Access Name`
The name of the access on which this VC resides.

`LCN index`
The index assigned to the VC LCN.

`Permanent Virtual Circuit or Switched Virtual Circuit`
Identifies the type of VC in use.

`Local Address`
The local DTE X.121 address.

`Remote Address`
The remote DTE X.121 address.

`# Packets Sent count`
The number of X.25 data packets sent.

`# Packets Received`
The number of X.25 data packets received.

`# Resets Sent count`
The number of times the local DTE reset the VC.

`# Resets Received`
The number of times the network or remote DTE reset the VC.

`# RR Sent count`
The number of receive ready packets sent.

`# RR Received`
The number of receive ready packets received.

RNR Sent count
The number of receive not ready packets sent.

RNR Received
The number of receive not ready packets received.

Bytes Sent Count
The total number of data bytes sent since the last reset or restart.

Bytes Received
The total number of bytes received since the last reset or restart.

ROUTINE MAINTENANCE

OVERVIEW

The information in this chapter provides instructions for performing routing maintenance on the CyberSWITCH. The information falls into the following categories:

- installing / upgrading system software
- executing configuration changes
- performing a configuration backup and restore
- obtaining system custom information

INSTALLING/UPGRADING SYSTEM SOFTWARE

System software is delivered on 3.5" high-density diskettes. For details regarding your specific software version, view the System Release Notes by issuing the `list rel_notes.txt` command. For installation and / or upgrade details, refer to *Upgrading System Software*.

EXECUTING CONFIGURATION CHANGES

There is a configuration utility, CFGEDIT, and a dynamic management mechanism, Manage Mode, which may be used together to execute configuration changes. The following sections briefly describe these tools. For a detailed explanation of the configuration process, refer to *Configuration Tools*. For information on configuration elements, refer to the configuration chapters of this guide.

CONFIGURATION FILES

The system maintains configuration information in four separate configuration files, which are located in the system's `\config` directory. These files are:

- network.nei
- node.nei
- devdb.nei
- lan.nei
- ip.nei
- platform.nei

For more details on these and other system files, refer to the *Software Overview* chapter.

MAKING CHANGES USING CFGEDIT

If you need to make changes to the system's configuration, you can change the configuration files using the run-time configuration utility, CFGEDIT. To begin, you must have an active administration session up. Then, enter the following command at the system prompt:

```
cfgedit
```

As long as there is no other "change" session active (CFGEDIT or Manage Mode), you will have access to the configuration editor. Make the required configuration changes. Note that these

changes are NOT dynamic. The changes are saved in a temporary copy of configuration data, and will not affect the current run-time operation of the system in any way.

To terminate the session, return to the main CFGEDIT menu. Select the *save changes* option. Then press <RET> to exit.

Note: This "save" process also includes all unsaved Manage Mode changes which were made prior to the CFGEDIT session, if any.

At your earliest possible convenience, reboot the system. This will then activate the new configuration data. It is also wise to make a copy of the new configuration files, as described earlier.

MAKING CHANGES USING MANAGE MODE

In addition to CFGEDIT, you may use the Dynamic Management feature to make certain changes to configuration. The Manage Mode consists of a series of console commands that enable you to display current system parameters, change many parameters dynamically, and write changes to disk files so that they remain permanent.

To access Dynamic Management commands, enter the Manage Mode by typing the following command at the system prompt:

```
>manage
```

Once Manage Mode is active, the prompt changes from ">"to "MANAGE>". While operating in this mode, only Dynamic Management commands are available. All other system commands are ignored until you exit Manage Mode and return to the normal system command mode. To return to the system command mode, issue the following command:

```
MANAGE> exit
```

Available Manage Mode commands are dispersed throughout the configuration chapters. Refer to the *Manage Mode Command Table* for a complete listing of Manage Mode commands.

CONFIGURATION BACKUP AND RESTORE

After making configuration changes, back up the new configuration, either to diskette or network management station. To accomplish this, use TFTP to copy the configuration data (\system*.nei) from one machine to another. For more information on TFTP, refer to the *Remote Management* chapter.

To restore a configuration, use TFTP to transfer the configuration files back to the system. Then restart the system for the new configuration to take effect.

OBTAINING SYSTEM CUSTOM INFORMATION

If diskettes are included with your system, the labels affixed to the System Diskettes specify customized information for that copy of the system software, which may include: Version, Serial Number, Variant, Release and Options. Once this software is installed on the system, it is possible to obtain this information from the Administration Console when the system is running by issuing the `ver` command at the system prompt. The customized information for the system software will then be displayed.

APPENDICES

The *User's Guide* includes the following appendices:

- *System Worksheets*
  We have designed a set of worksheets you can fill out before you begin your CyberSWITCH configuration. Once filled out, they will contain information you will need for the configuration process.

- *CFGEDIT Map*
  A CFGEDIT map you can use as an aid when configuring your system. As you proceed through the configuration process, this map can help you understand where you are in the CFGEDIT structure.

- *Getting Assistance*
  Includes a System Problem Report you can use to inform us of any difficulties you have with our products.

- *System Adapters*
  Illustrates the various system adapters, highlighting appropriate jumpers and switch blocks on each board.

- *System Commands*
  A table that lists all system administration commands (including both Administrative and Guest commands).

- *Manage Mode Commands*
  A table that lists all of manage mode commands (used for dynamic management).

- *Cause Codes*
  A table that provides Q.931 cause codes and their corresponding meanings. Cause codes may appear in Call Trace Messages.

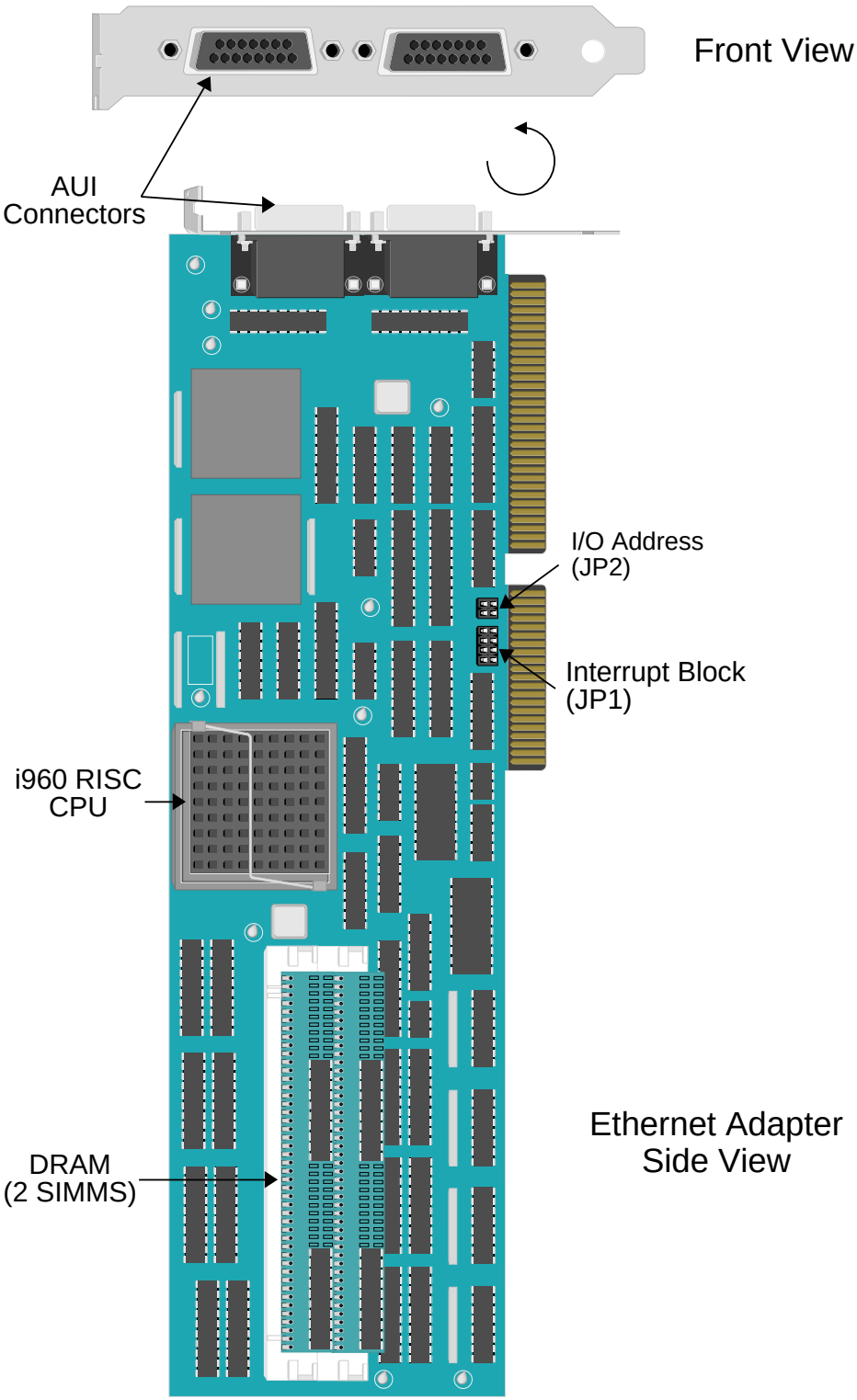
SYSTEM ADAPTERS

This appendix includes the following illustrations of available CyberSWITCH adapters:

- *Ethernet*
- *Basic Rate*
- *Primary Rate:*
  - *PRI-8*
  - *PRI-23*
  - *PRI-23/30*
- *Expander*
- *V.35*
- *RS232*
- *Digital Modem*
  - *DM-8*
  - *DM-24*
  - *DM-24+/DM-30+*
- *Encryption: DES (USA)*

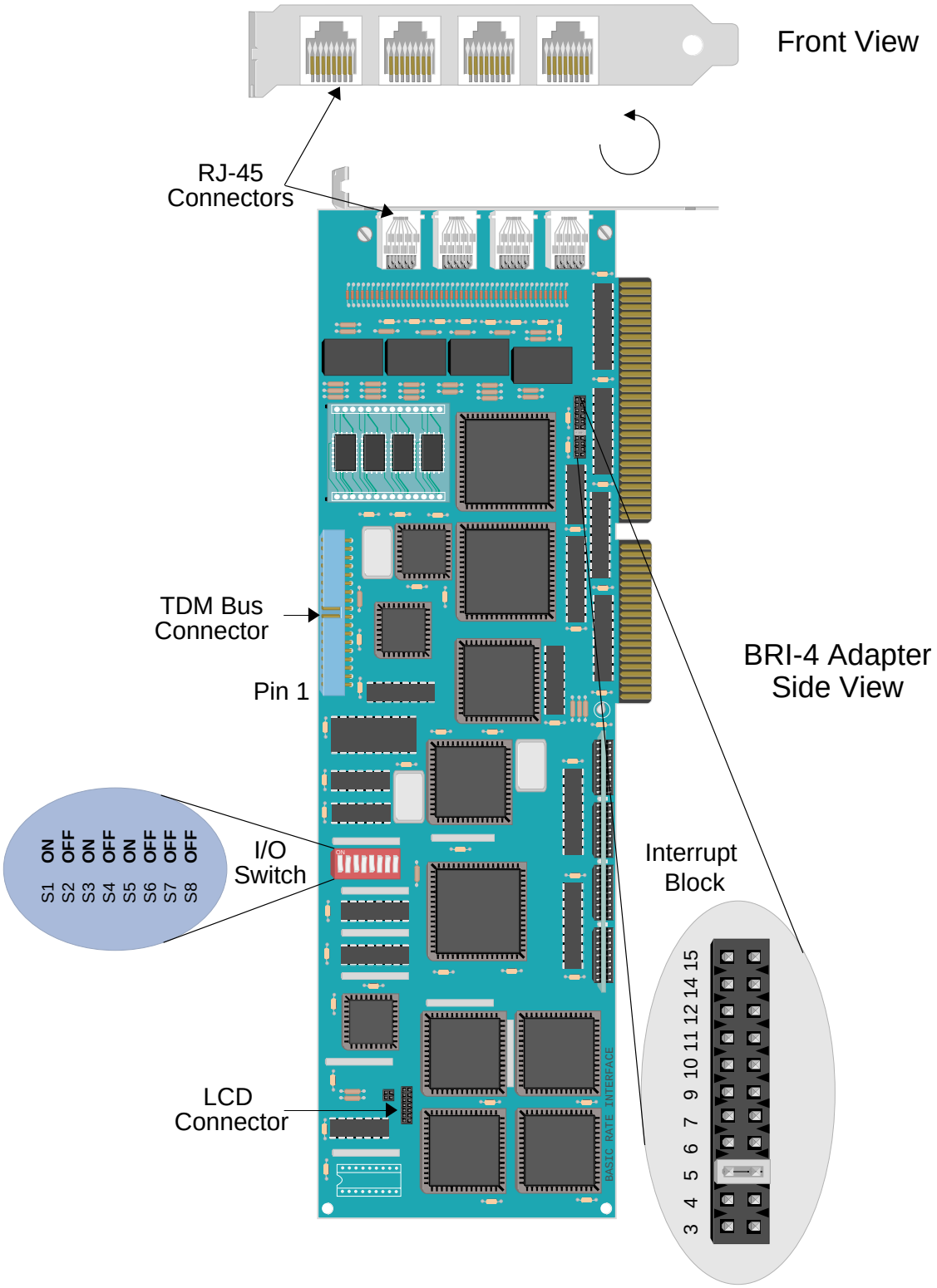
Generally, adapter switch settings are preset and adapters are preinstalled prior to shipment. However, in the event you need to do any part of this installation on-site, you must determine the correct switch settings for the adapters in question. Refer to *Adapter Settings* in the *Hardware Installation* chapter as well as referring to the illustrations in this appendix.

ETHERNET ADAPTER



BASIC RATE ADAPTER

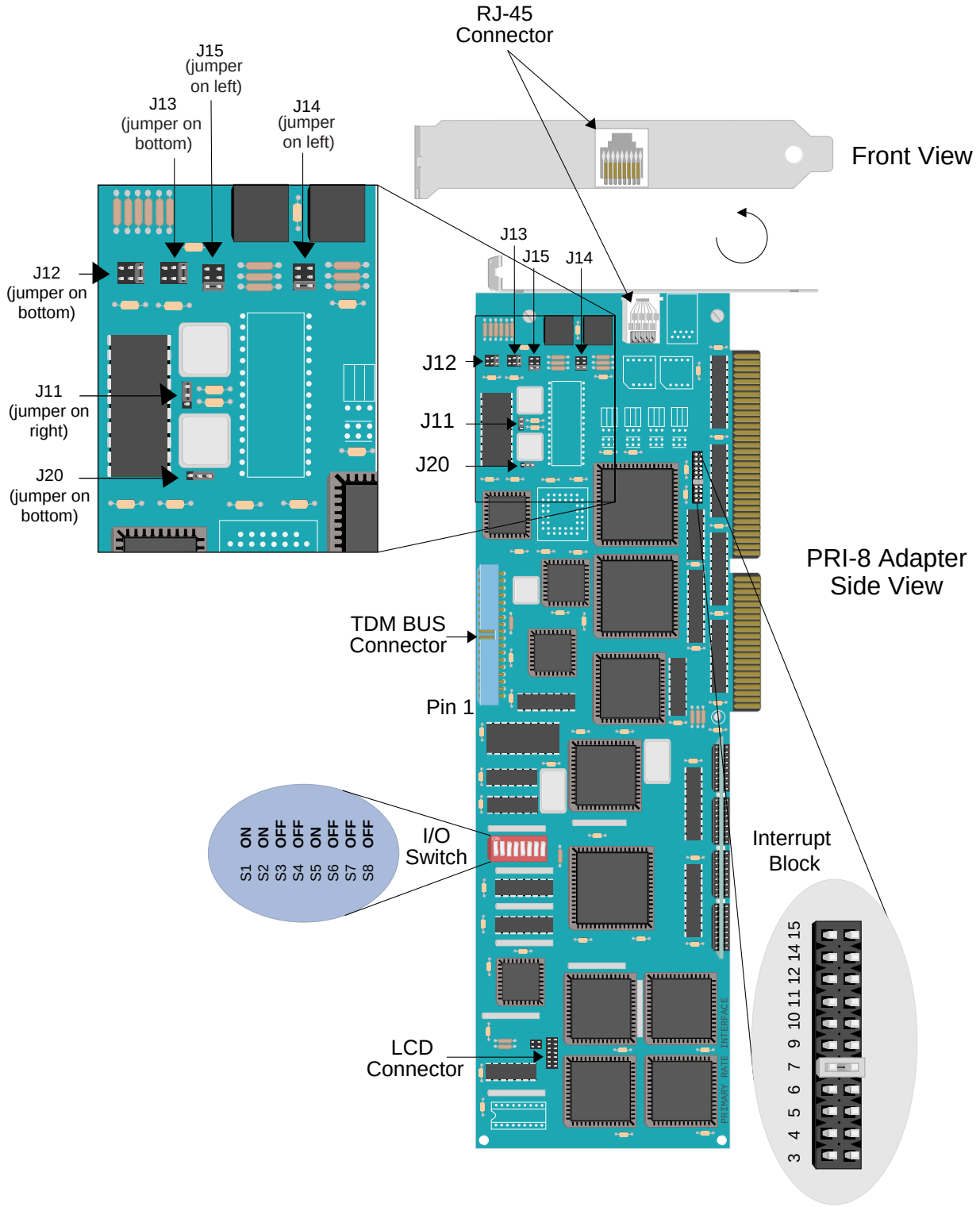
This adapter is set for slot 3:



PRIMARY RATE ADAPTERS

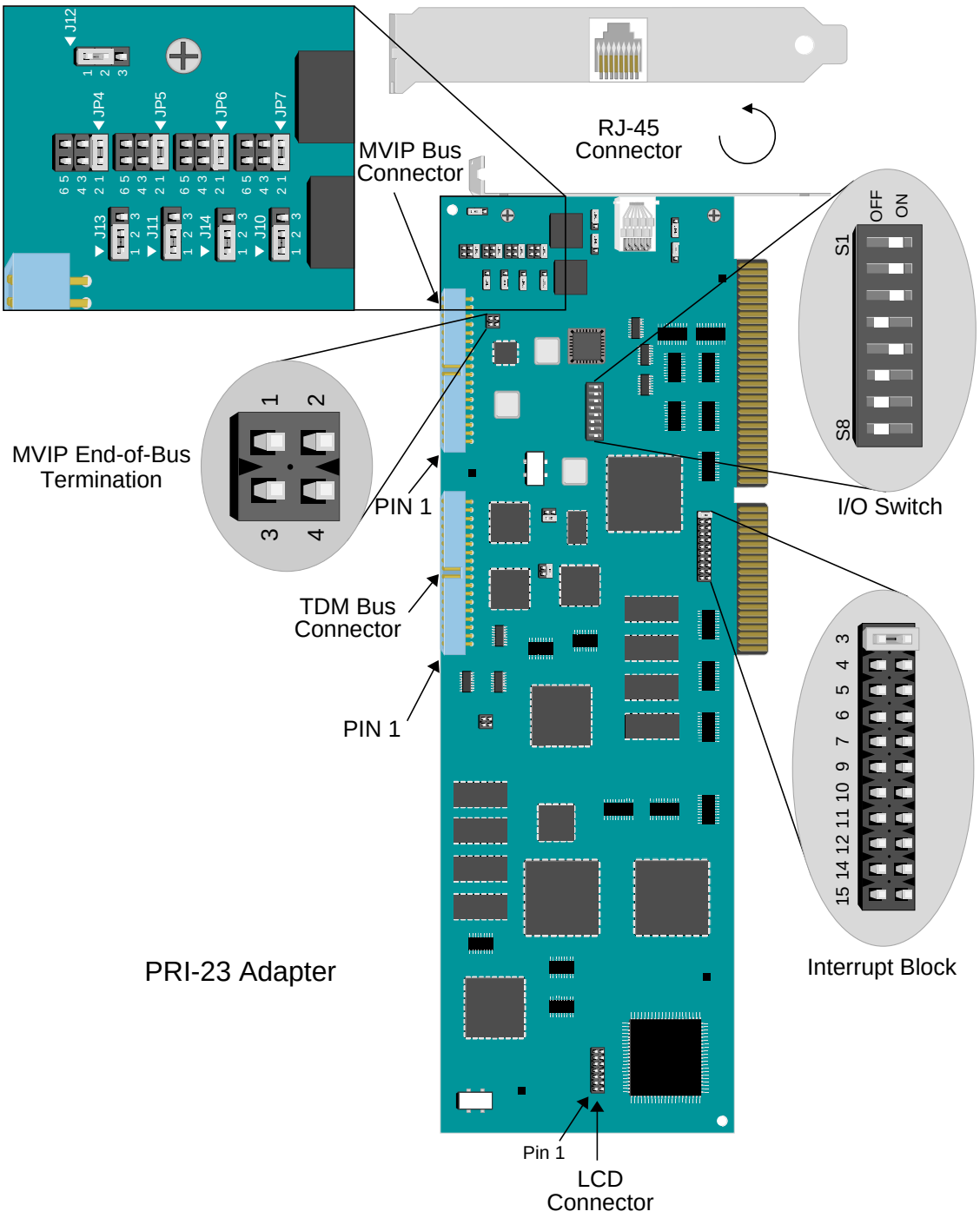
THE PRI-8

This adapter is set for slot 5:



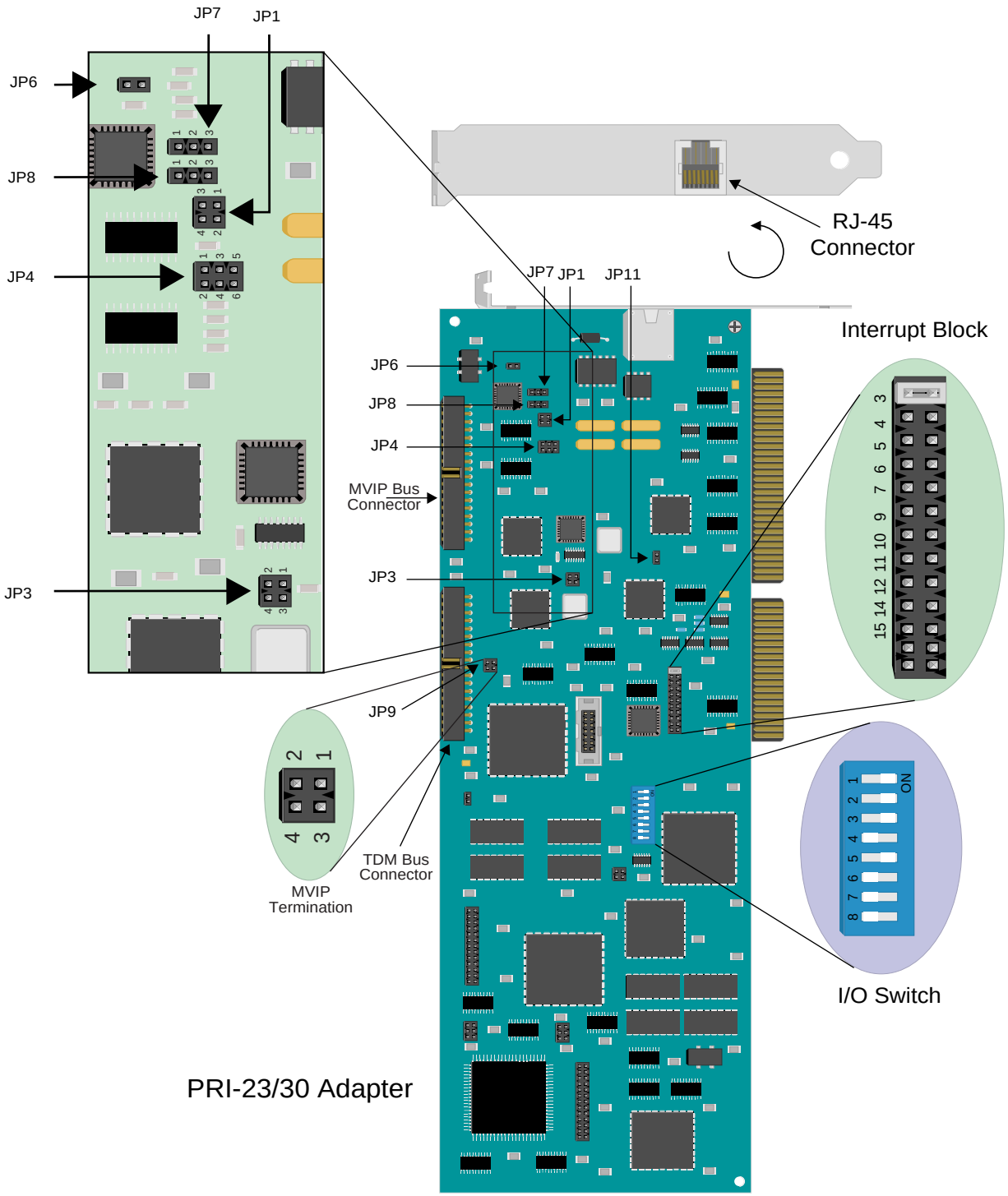
THE PRI-23

This adapter is set for slot 1:



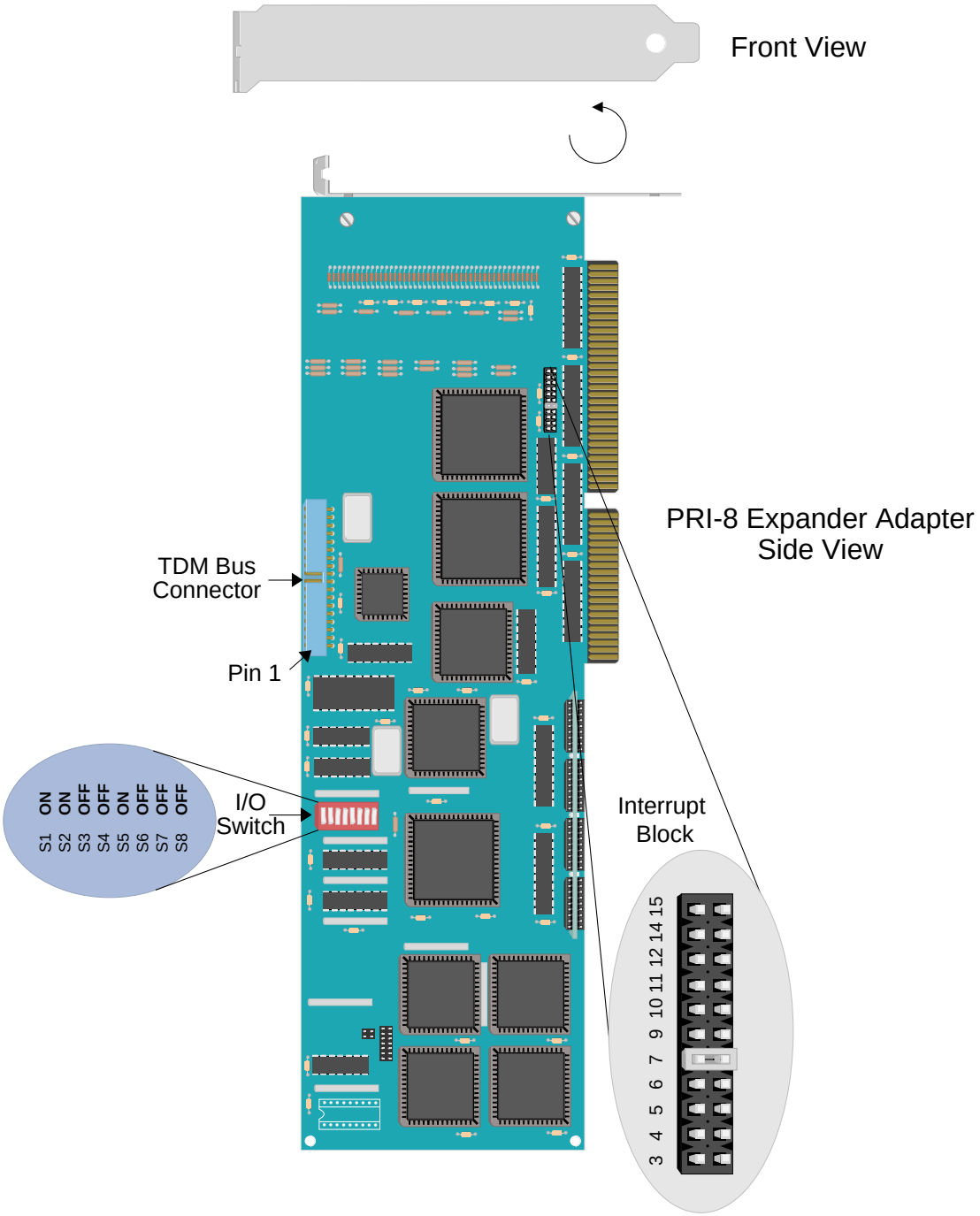
THE PRI-23/30

This adapter is set for slot 1. Note that S8 on the I/O Switch is not used. The board should function properly with the switch in either the ON or OFF position.



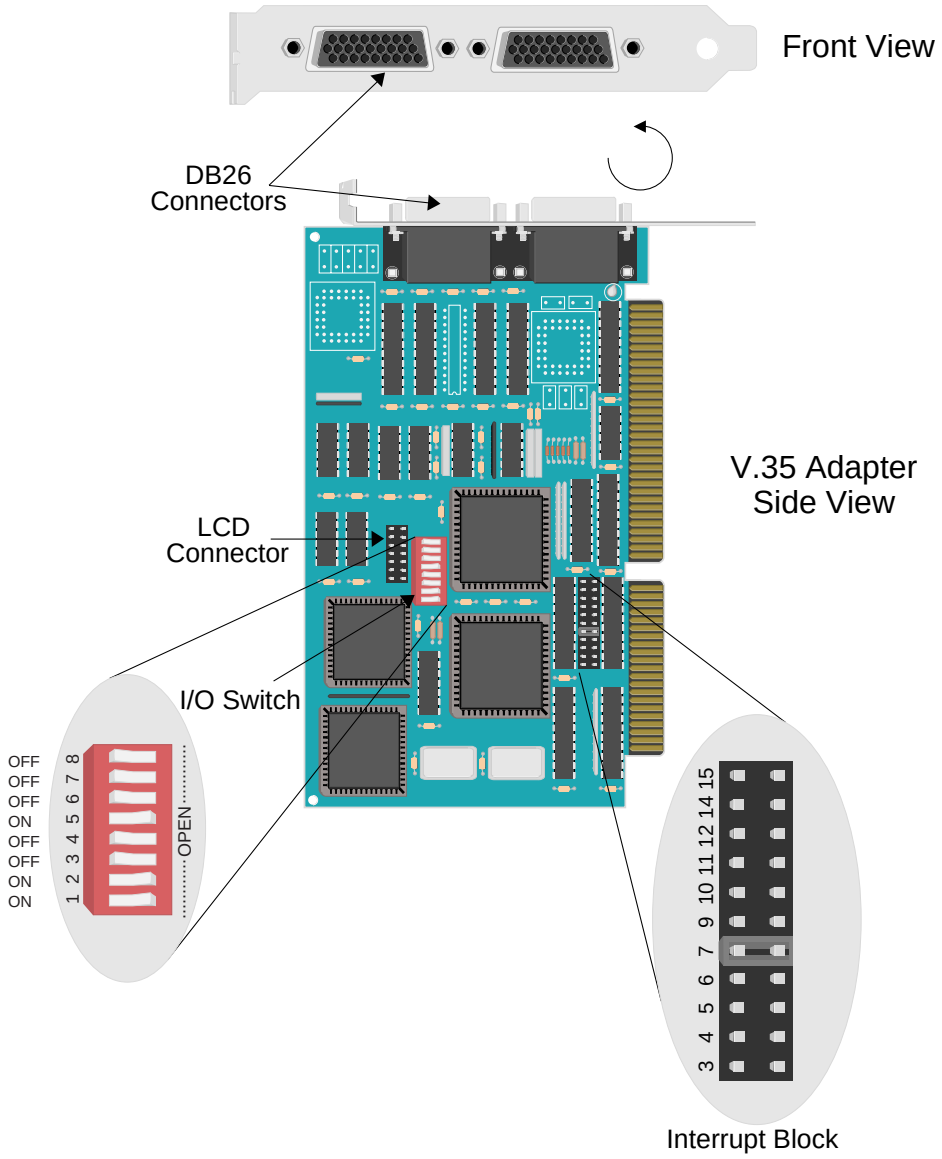
EXPANDER ADAPTER

This adapter is set for slot 5:



V.35 ADAPTER

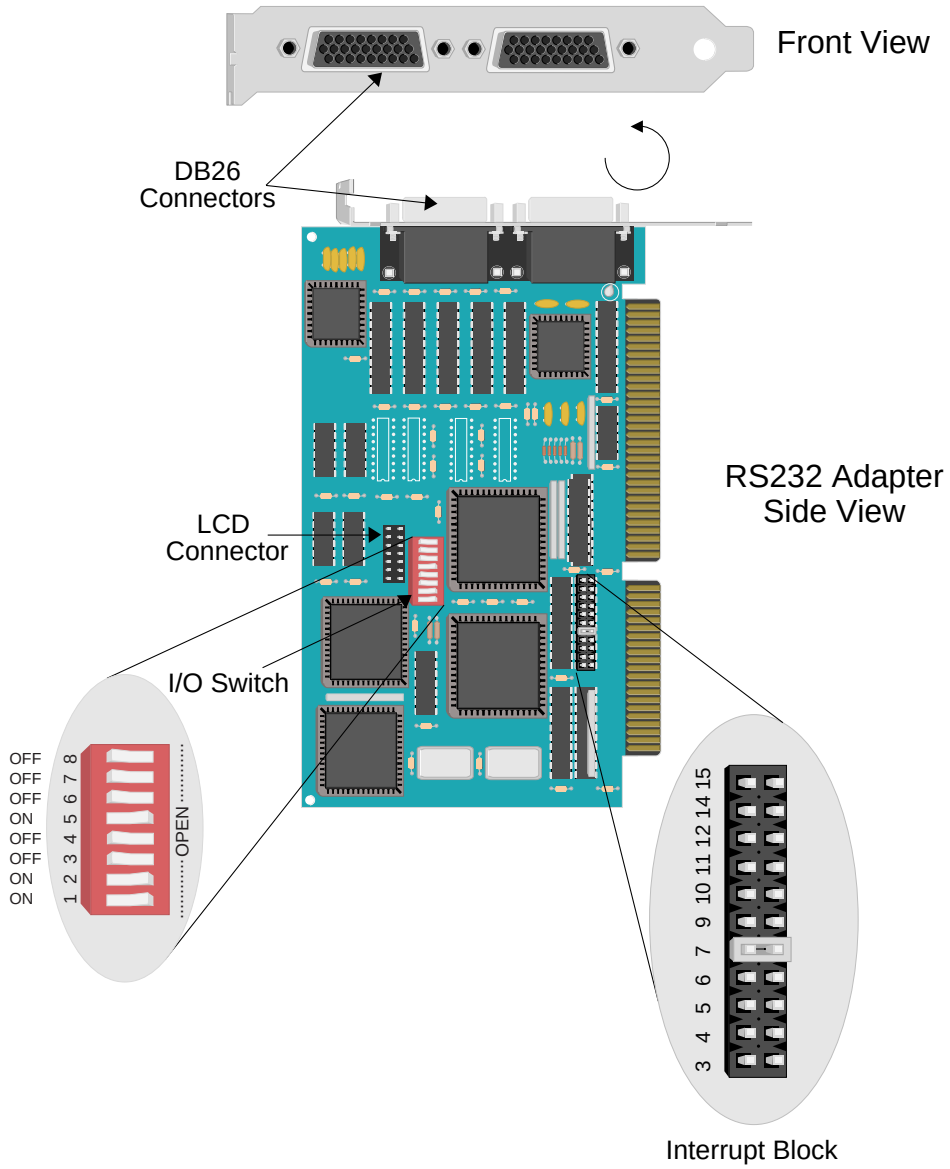
This adapter is set for slot 5:



Note: Switch label “OPEN” is the same as OFF on I/O switch.

RS232 ADAPTER

This adapter is set for slot 5:

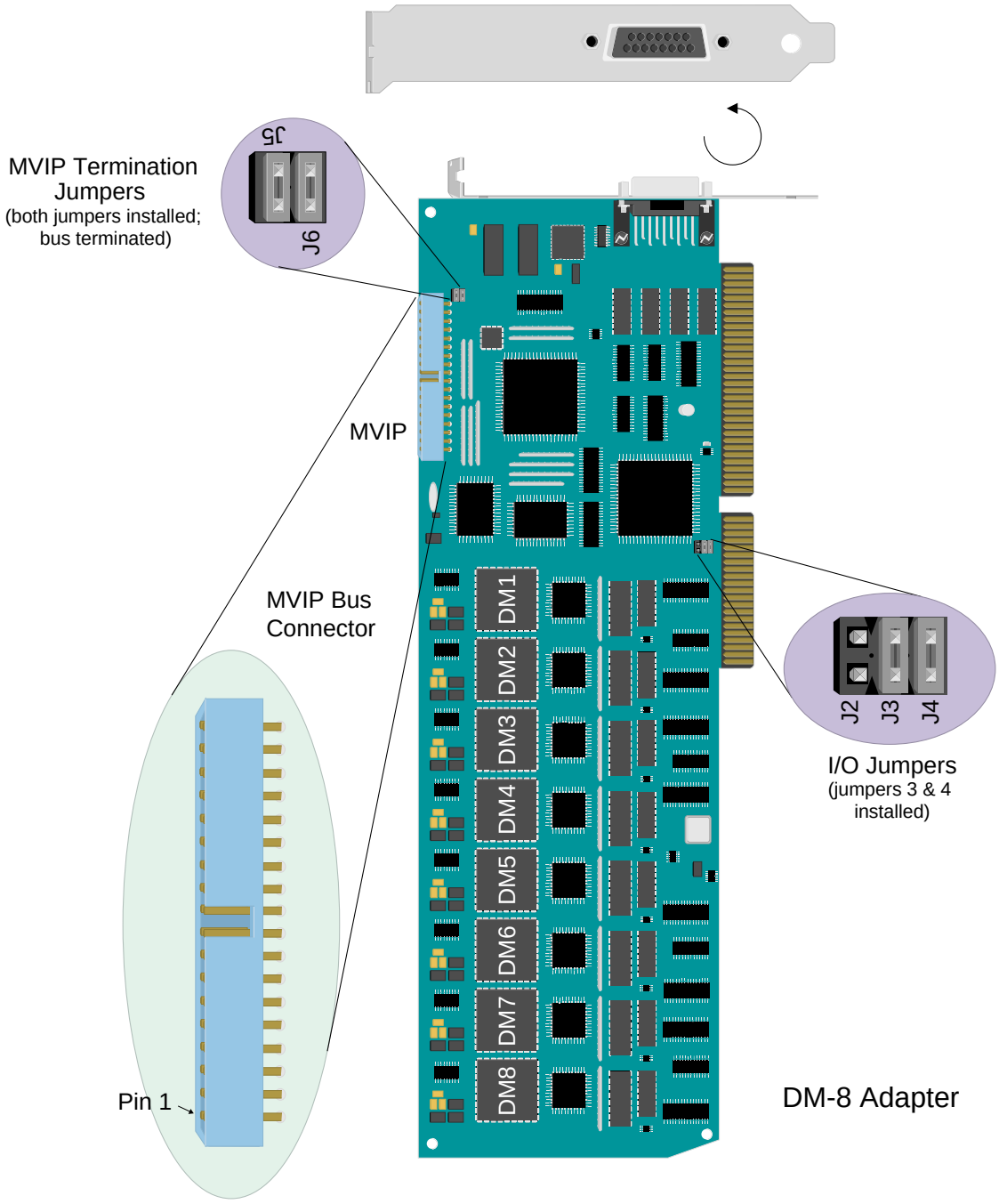


Note: Switch label "OPEN" is the same as OFF on I/O switch.

DIGITAL MODEMS

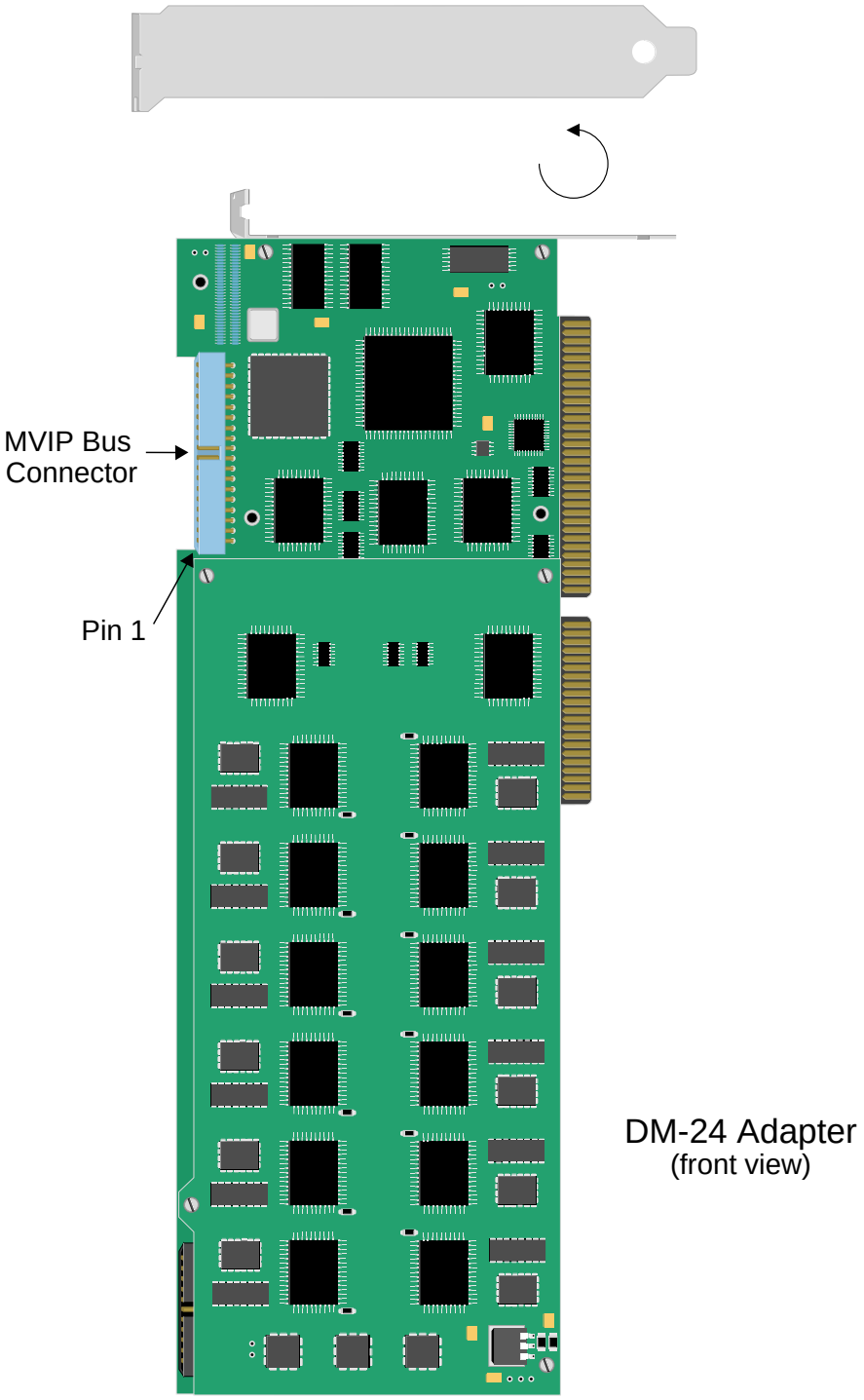
THE DM-8

This card is configured as the second DM-8 in the system as well as the last card on the MVIP bus:



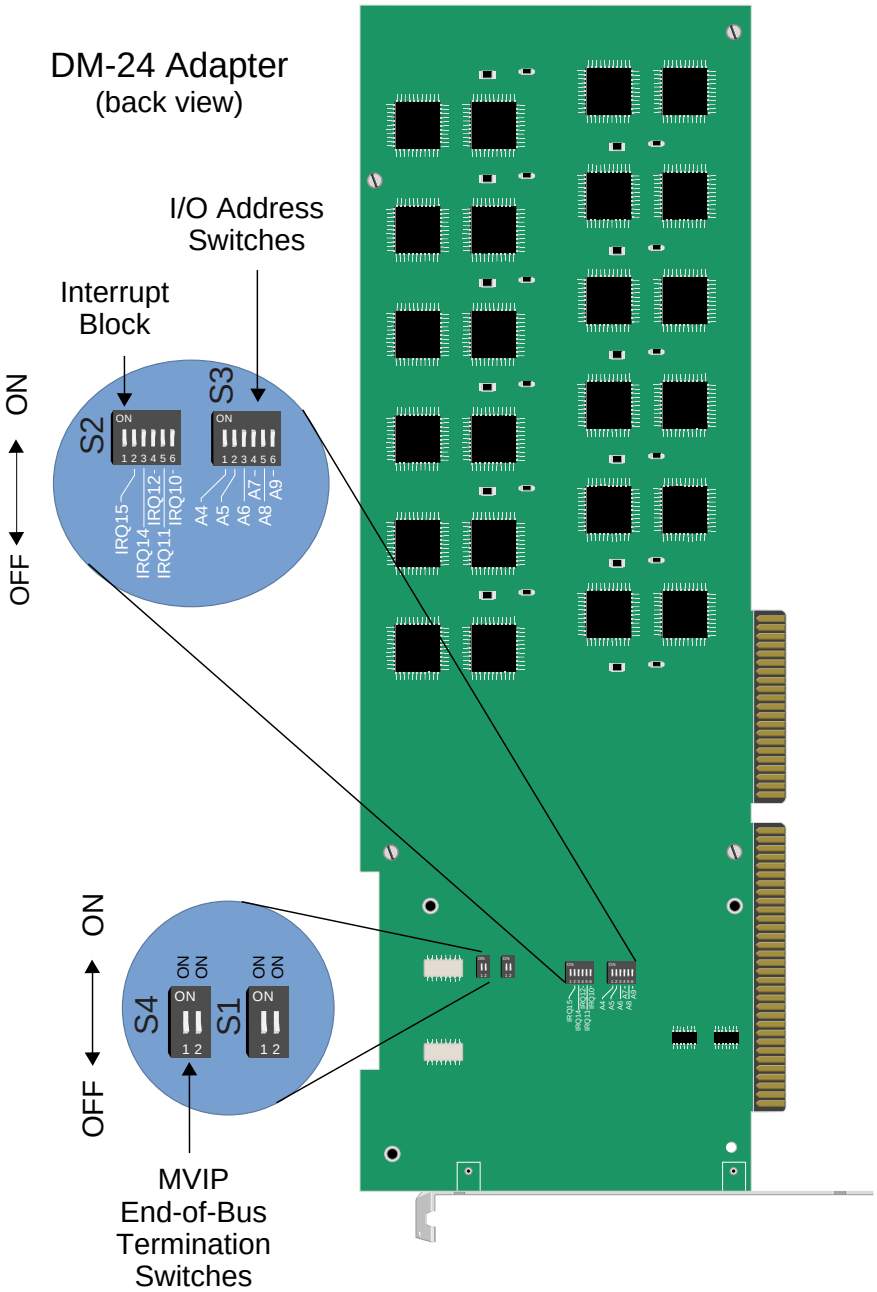
THE DM-24

The DM-24 adapter consists of a mother board / daughter board combination; daughter board sets on top of larger mother board. **Front of board**:



DM-24 Adapter
(front view)

DM-24, back view (Illustration does not depict switches set for any particular slot):

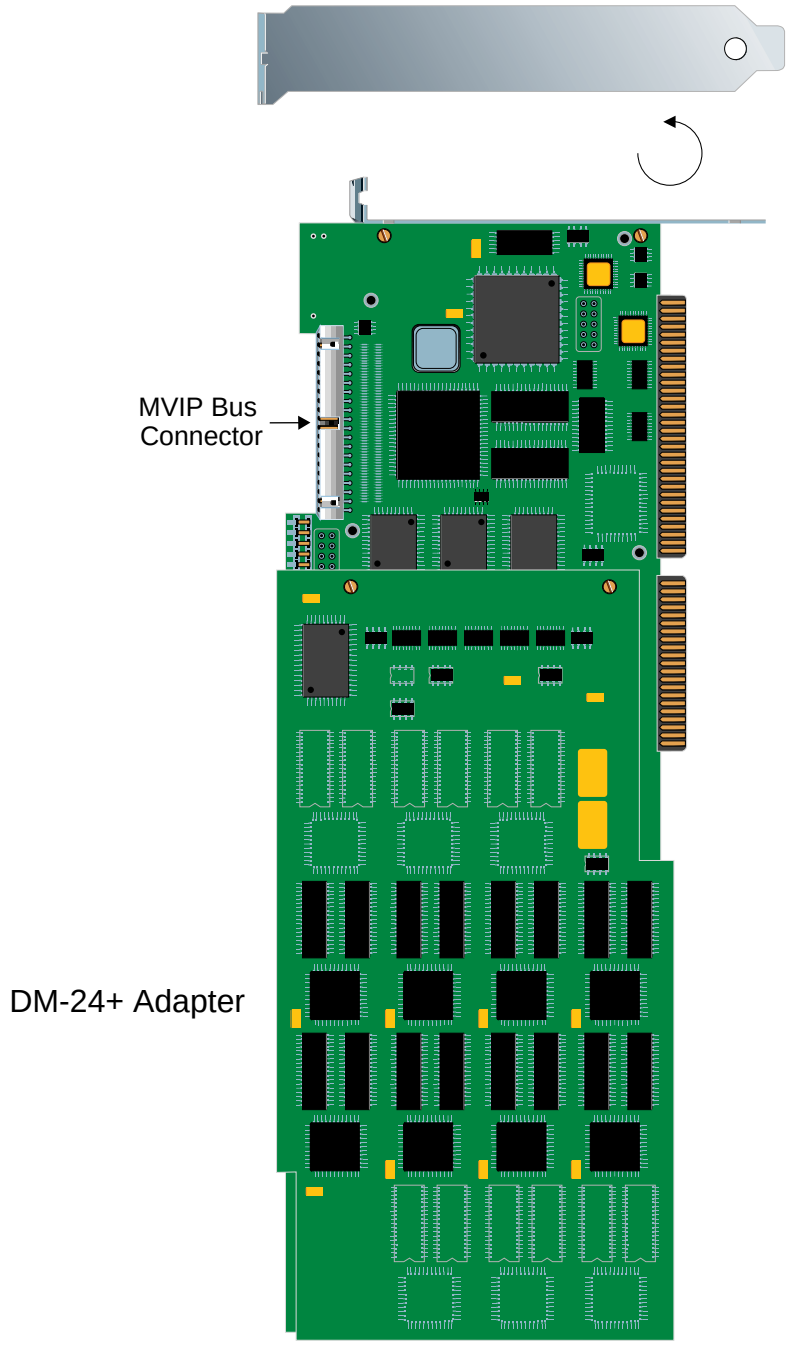


Note: In rare cases, there may be some variation with silk screening from card to card. “ON” and “1”/”2” may be labeled on opposite sides of the switch, but the “ON” switch position is always to the right (as illustrated above).

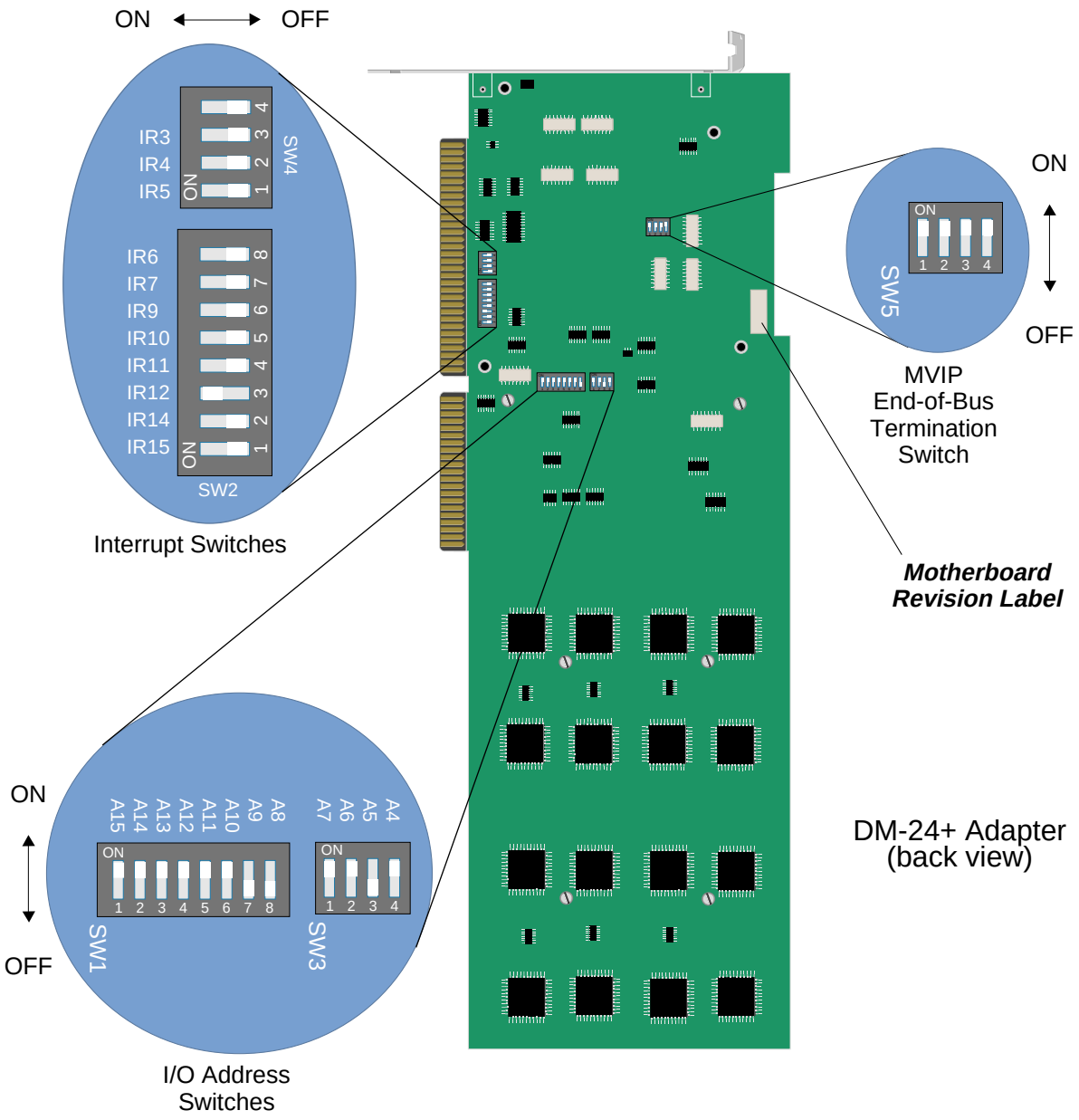
If your card uses the labeling DIS/EN or =1/=0, note the following: For IRQ, “off” is the same as DIS (disabled); “on” is the same as EN (enabled). For I/O address, “off’ is the same as “1”; “on” is the same as “0”.

THE DM-24+/DM-30+

The DM-24+ and the DM-30+ adapters consist of a mother board / daughter board combination. The two adapters closely resemble each other, but are distinguishable by the number of modems each supports. There are 30 modem chips on the DM-30+; and 24 modem chips on the DM-24+.

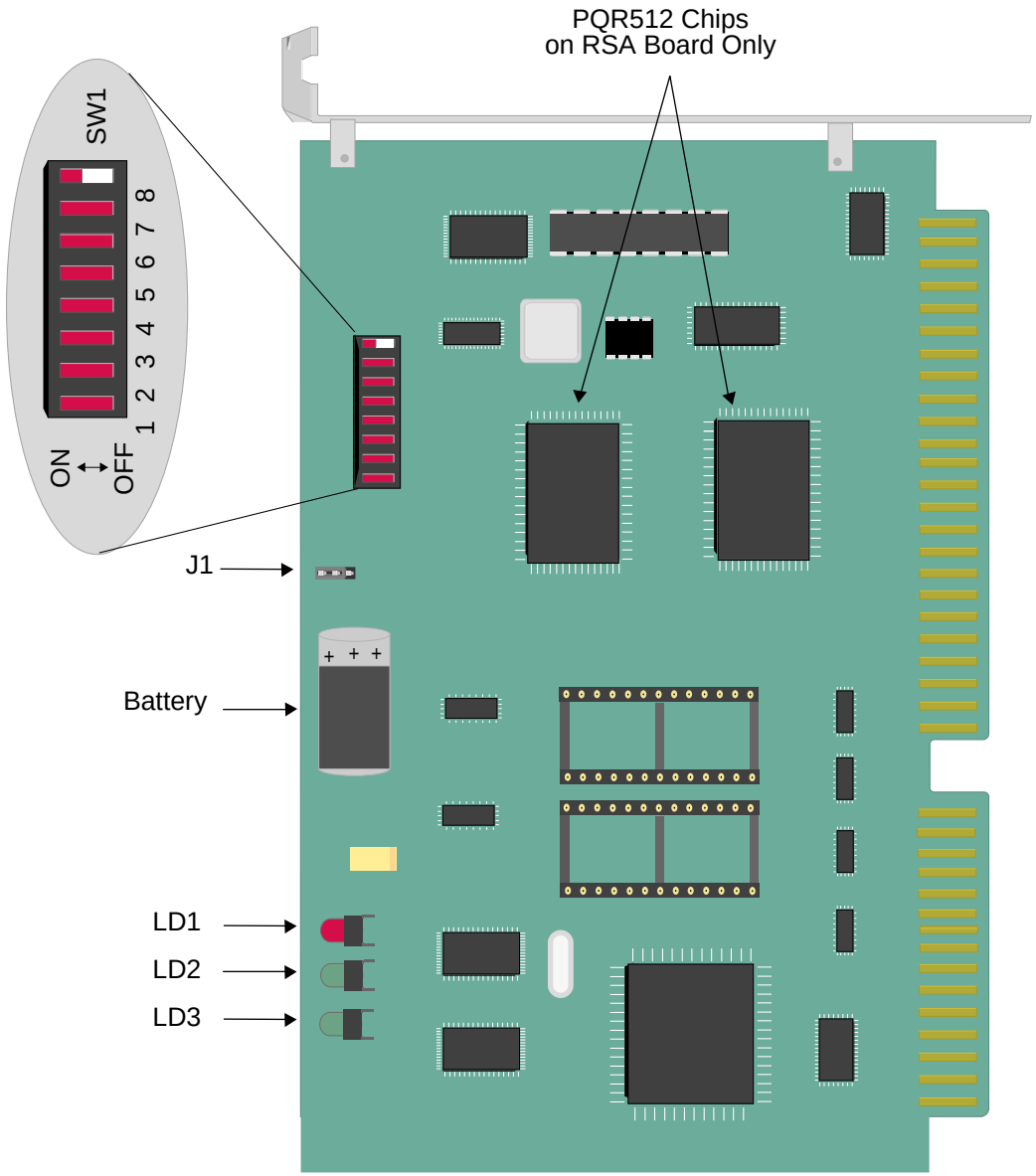


Pertinent switches are located on the back side of the mother board. The following illustrates switch settings for a **DM-24+** board in slot 6:



ENCRYPTION ADAPTER

DES ADAPTER (US VERSION)



RSA/DES Adapter (USA)

Note: Jumper J1 *must be installed* for the board to be operational.

SYSTEM WORKSHEETS

The worksheets included in this appendix will be helpful in configuring and managing your system. They capture important network information. To see examples of completed worksheets, refer to the *Example Networks Guide*.

Worksheets included in this appendix are:

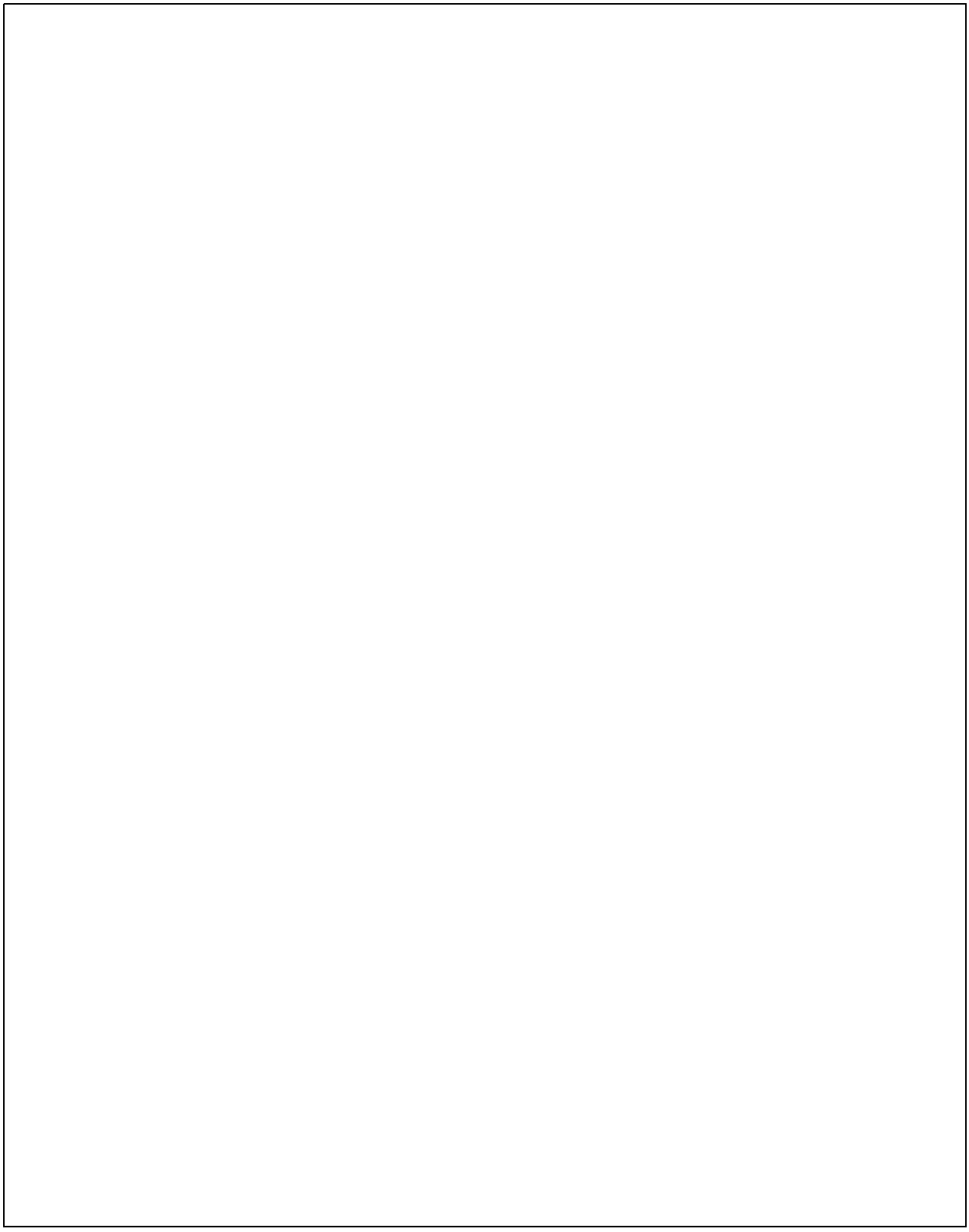
1. Network Topology Worksheet. This worksheet identifies the following information:
   - The Users or Remote Sites in your network.
   - The telephone numbers associated with the Users or Remote Sites in your network.
   - IP/IPX/AppleTalk information related to the Users or Remote Sites in your network.
   - Bridge addresses related to the Users or Remote Sites in your network.
   - Password information related to the Users or Remote Sites in your network.

2. System Details Worksheet. This worksheet identifies the following information for each CyberSWITCH in your network:
   - The resource details for each adapter in your CyberSWITCH. Note the switch type.
   - Details on each ISDN line attached to your CyberSWITCH. If a line has more than one SPID, use an extra worksheet line to record that SPID and its associated directory number.
   - Details on any configured accesses.

3. The Device Information Worksheet identifies device information for one device. Complete a worksheet for each of your network's remote devices.

4. Use the Bridging and Routing Information Worksheets to summarize your particular setup (from the Network Topology Worksheet) to ease the configuration process.

NETWORK TOPOLOGY



SYSTEM DETAILS

System Name: _____ PAP Password:_____ CHAP Secret:_____

RESOURCES

Type	Slot	Switch type	Synchronization type

LINES

BRI Lines

Name	Slot	Port	Line type	Call screen	TEI	SPID	Directory number

PRI Lines

Name	Slot	Port	Framing type	Line coding	Sig. method	Line build-out

V.35 and RS232 Lines

Name	Slot	Port	Device/Network	Idle character

ACCESSES

Dedicated Accesses

Over ISDN:

Line name	Data rate	Bearer channels	Line protocol	Device tied to this access
	❒ 56 Kbps ❒ 64 Kbps			
	❒ 56 Kbps ❒ 64 Kbps			
	❒ 56 Kbps ❒ 64 Kbps			
	❒ 56 Kbps ❒ 64 Kbps			

Over Serial connection:

Line name	Clocking	Data rate	Line protocol	Device tied to this access
	❒ Internal ❒ External			
	❒ Internal ❒ External			
	❒ Internal ❒ External			
	❒ Internal ❒ External			

X.25 Accesses

Over ISDN:

Line name	Access name	X.121 address of local DTE	Data rate	Bearer channels	Virtual circuits (PVCs)

Over serial connection:

Line name	Access name	X.121 address of local DTE	Clocking	Data rate	Virtual circuits (PVCs)
			❒ Internal ❒External		

Frame Relay Accesses

Over ISDN:

Line name	Access name	Data rate	Bearer channels	DLCI	PVC name	CIR	EIR
		❒ 56 Kbps ❒ 64 Kbps					

Over serial connection:

Line name	Access name	Clocking	Data rate	DLCI	PVC name	CIR	EIR
		❒ Internal ❒ External					

DEVICE INFORMATION

Device Name: _____

Calling (ISDN, FR, etc.) Information

Line Protocol	
Base Data Rate	
Initial Data Rate	
Max Data Rate	
Dial-Out Number(s)	

X.25 Information

PVC	
SVC	

Authentication Information:

PAP Password	
CHAP Secret	
IP Host ID	
Bridge Ethernet Address*	
Bridge Password*	
CLID(s)	

Frame Relay Information

DLCI	

* HDLC Bridge only

Protocol for this particular device?

Bridge

Bridging enabled?	❒ enabled ❒ disabled
Make calls for bridged data?	❒ enabled ❒ disabled
For IP RLAN, IP (Sub-) network number	
For IPX RLAN, external network number	

IP

IP enabled?	❒ enabled ❒ disabled
IP Address (on WAN link)	❒ 0.0.0.0 if unnumbered link
Make calls for IP data?	❒ enabled ❒ disabled
IP input filter?	
IP output filter?	

IPX

IPX enabled?	❒ enabled ❒ disabled
Callable by IPX?	❒ enabled ❒ disabled
IPXWAN protocol?	❒ enabled ❒ disabled
IPX routing protocol?	❒ none ❒ RIP/SAP ❒ triggered RIP/SAP
IPX spoofing?	

AppleTalk

AppleTalk enabled?	❒ enabled ❒ disabled
AppleTalk Address	
Make calls for AT data?	❒ enabled ❒ disabled
AT Routing Protocol	

BRIDGING AND ROUTING INFORMATION

BRIDGING

Bridging	❒ enabled	❒ disabled
Mode of Operation	❒ restricted	❒ unrestricted
Bridge Filters		
Bridge Dial Out/ Known Connect List		

IP ROUTING

IP Routing	❒ enabled	❒ disabled
Mode of Operation	❒ router	❒ IP host

Network Interface Information

LAN	Name			
	IP address			
	Mask			
Unnumbered WAN	❒ need ❒ don't need			
	Input filters			
	Output filters			
Remote LAN	Name			
	IP address			
	Mask			
	Input filters			
	Output filters			
Traditional WAN	Name			
	IP address			
	Mask			
	Input filters			
	Output filters			
Direct Host WAN	Name			
	IP address			
	Mask			
	Input filters			
	Output filters			
IP Host Mode	IP address			
	Mask			
	Input filters			
	Output filters			

IP ROUTING, CONTINUED

Static Routes

Destination network address	Mask	Next hop
❒ default?		
❒ default?		
❒ default?		
❒ default?		

IPX ROUTING

Routing Information

IPX routing	❒ enabled ❒ disabled
Internal network number	

Network Interface Information

LAN	Name			
	External network number			
Remote LAN	Name			
	External network number			

Static Routes

Destination network number	Next hop
❒ Int. ❒ Ext.	
❒ Int. ❒ Ext.	
❒ Int. ❒ Ext.	
❒ Int. ❒ Ext.	
❒ Int. ❒ Ext.	
❒ Int. ❒ Ext.	

NetWare Static Services

Service name	Type	Internal network number	Node number	Socket number

APPLETALK ROUTING

AppleTalk Routing/Port Information

AppleTalk routing	❒ enabled	❒ disabled		
LAN	Name			
	Port number			
	Network type	❒ extended ❒ nonextended		
	Netwk range/ number			
	AppleTalk address			
	Zone name(s)			
WAN	Name			
	Network type	❒ extended ❒ nonextended	❒ extended ❒ nonextended	❒ extended ❒ nonextended
	Netwk range/ number			
	AppleTalk address			
	Zone name(s)			
Unnumbered WAN	❒ need ❒ don't need			
MAC Dial In WAN	Network type	❒ extended ❒ nonextended	❒ extended ❒ nonextended	❒ extended ❒ nonextended
	Netwk range/ number			
	AppleTalk address			
	Zone name(s)			
WAN (Remote LAN)	Name			
	Network type	❒ extended ❒ nonextended	❒ extended ❒ nonextended	❒ extended ❒ nonextended
	Netwk range/ number			
	AppleTalk address			
	Zone name(s)			

AppleTalk Port Static Routes

Network type to be accessed	Destination network range	Next hop address	Next hop name	Number hops	Zone name(s)
❒ extended ❒ nonextended					
❒ extended ❒ nonextended					

CFGEDIT MAP

OVERVIEW

The following pages provide an outline of the CyberSWITCH CFGEDIT configuration utility. As you configure your system, you may find it helpful to use this outline as a map to help you navigate through CFGEDIT.

MAIN MENU

Note: All options listed may not be available on your particular system. The availability of these options depends upon the platform and software you have ordered, as well as your configuration choices.

Physical Resources

- Resources
- Lines
- Accesses
- ISDN SubAddress

Options

- Bridging
- IP Routing
- IPX
- AppleTalk Routing
- SNMP
- PPP
- Call Control
- Default Line Protocol
- Default Async Protocol
- Log Options
- Compression
- FR DBU
- RADIUS Accounting

Security

- Security Level
- System Options and Information
- Device Level Databases
- User Level Databases (Enable / Disable)
- Off-node Server Information
- Network Login Information

PHYSICAL RESOURCES MENU

RESOURCES

- COMMPORT
- Basic Rate
  - switch type
- T1/E1/PRI
  - switch type
  - synchronization
- Expander
- V.35
- RS232
- Ethernet 1, 2
- Digital Modem 8, 24, 30
  - mu law
  - A-law
- DES-RSA

DATA LINES

- ASYNDMPORT
- Name/Slot/Port/Framing/Line coding/Signalling/Line build out
- Datalinks
  - PPP: TEI negotiation
  - PMP: Call Screen Method
    - name
    - subaddress
    - telephone number

ACCESSES

- Dedicated
  - Data rate
  - Bearers list
  - Line protocol
    - HDLC
    - PPP
    - FR DBU
  - Device name
- X.25
  - Name
  - Data rate
  - X.121 address
  - BPS
  - Bearers list
  - LAPB info
  - VC
- Frame Relay
  - Data rate
  - Bearers
  - Access info
  - PVCs

OPTIONS MENU

BRIDGING

- Enable / Disable
- Spanning Tree
- Mode of Operation
  - unrestricted, restricted
- Bridge Filters
  - protocol definition
  - filters (source, destination, protocol, packet data)
- Known Connect List

IP ROUTING

- Enable / Disable
- IP Operating Mode (host / router)
- Interfaces
  - LAN
  - WAN
  - WAN (Direct Host)
  - WAN (RLAN)
  - WAN (unnumbered)
  - IP Host
- Static Routes
- RIP (enable / disable)
- Static ARP table
- Isolated Mode (enable / disable)
- Static Route via RADIUS
- IP Address Pool
- IP Filters
  - Packet Type
    - Source, Destination,
    - Protocol
  - Forwarding Filters
  - Connection Filters
  - Exception Filters
  - Application
- DHCP
  - Relay Agent
    - hop count
    - destination IP address
  - Proxy Client
    - maximum # addresses
    - IP addresses to prefetch
    - LAN port
- NBNS and DNS name server addresses
- IP Security Associations
  - Packet direction
  - Destination / source IP addresses
  - Initial value length
  - Shared secret encryption key
  - Security Association Authentication
  - SPI

IPX ROUTING

- Enable / Disable
- IPX Network Number
- IPX Interfaces
  - LAN
  - Remote LAN
- Routing Protocols
  - IPX RIP, IPX SAP
  - number table entries
- IPX Static Routes
  - RIP info
  - number of ticks, hops
  - next hop
  - destination IPX number
- Netware Static Services
  - SAP info
  - number of hops to service
  - service IPX socket number
  - service IPX node number
  - service IPX network number
  - service type
  - service name
- IPX Spoofing
  - IPX, SPX watchdog
  - serial packet handling
  - message packet handling
- Type 20 Protocol
  - change devices
  - enable WAN forwarding
- Isolated Mode (enable / disable)
- Triggered RIP / SAP
  - WAN peer list display
  - RIP / SAP timers

APPLETALK ROUTING

- Enable / Disable
- Port information
- Static Routes
- Capacities
- Isolated Mode

SNMP

- Enable / Disable
- Community info
- Trap info
  - B-channel usage
  - authentication failures
- MIB2 group objects

PPP

- Global options
- LCP options
- IPCP options
- Link failure options

CALL CONTROL

- Throughput Monitor
- Call Interval
- Monthly call charges
- Call Restrictions
- Device Profile
- Bandwidth Reservation
- Semipermanent Connection
- Connection Services Manager (CSM) for Call Control
  - enable / disable
  - TCP port number
- D-Channel Callback
- Digital Modem Inactivity Timeout
  - enable / disable
  - timeout value (in minutes)

DEFAULT LINE PROTOCOL

- Action Timeout
- Timeout Value

DEFAULT ASYNC PROTOCOL

- Action on data timeout
- Use PPP protocol / use Terminal Mode
- Data timeout value

LOG OPTIONS

- Log Servers
- Call Detail Recording
- System Message (DR) log
- Authentication Message (DA) log

COMPRESSION

- Enable / Disable
- Default-per device
- PPP STAC-L25 sequence number

FR DBU

- Command / Control DLCI
- Outgoing data rate

SECURITY MENU

SECURITY LEVEL

- No Security
- Device Level Security
- User Level Security
- Device and User Level Security

SYSTEM OPTIONS AND INFORMATION

- System Options
  - PAP password
  - CHAP challenge
  - Bridge MAC address
  - IP Host ID
  - Calling Line ID
- System Information
  - system name
  - system password
  - system secret
- Administrative Session
  - Database Location
    - On-node
    - CSM
    - RADIUS
    - TACACS
    - ACE
  - Inactivity time-outs
  - Telnet admin sessions
  - TCP port number
  - Emergency Telnet port number

DEVICE LEVEL DATABASES

- On-node Device Database (Enable / Disable)
- On-node Device Entries (by name)
  - ISDN
    - line protocol
    - data rate
    - dial out numbers
    - subaddress
  - Frame Relay
  - X.25
    - SVC, PVC
  - Digital Modem
    - line protocol
    - baud rate
    - bearer capability
    - dial out numbers

Authentication
PAP password
CHAP secret
outbound authentication
user level authentication
IP host ID
bridge Ethernet
calling line ID
IP information
IP address
IP enable / disable
make calls for IP data
IPX
enable / disable
calls for IPX data
IPXWAN
IPX routing
none
RIP / SAP
trig RIP / SAP
IPX External WAN network number
IPX spoofing
AppleTalk information
AppleTalk address
enable / disable
make calls for AppleTalk data
AppleTalk routing protocol
Bridge information
IP (sub)network number
enable / disable
make calls
IPX network number
spoofing
Compression
PPP STAC-L25
Encryption
enable / disable
proprietary key exchange
decryption / encryption keys

- Off-node Device Database Location
  None (Use On-node)
  CSM
  RADIUS

USER LEVEL DATABASES (ENABLE/DISABLE)

- CSM
- RADIUS Authentication Server
- TACACS Authentication Server
- ACE Authentication Server

OFF-NODE SERVER INFORMATION

- CSM
  - TCP port
- RADIUS
  - Primary Server
  - Secondary Server
  - Miscellaneous info
    - number of retries
    - time between retries
- TACACS
  - Primary Server
    - IP Address
    - Shared Secret
    - UDP Port Number
  - Secondary Server
  - Miscellaneous info
    - number of retries
    - time between retries
    - packet format
- ACE
  - Primary Server
  - Secondary Server
  - Miscellaneous info
    - number of retries
    - time between retries
    - encryption method (SDI or DES)
    - source IP address
  - Load Server Configuration file
- RADIUS Accounting
  - Primary Server
    - IP Address
    - Shared Secret
    - UDP Port Number
  - Secondary Server
  - Miscellaneous info
    - number of retries
    - time between retries
- Miscellaneous Off-node Server Options
  - RADIUS Accounting (Enable / Disable)
  - RADIUS Type (RFC2138 / Cabletron)
  - Dynamic Device Option (Enable / Disable)
  - Dynamic Device Default Settings

NETWORK LOGIN INFORMATION

- Network login configuration (Terminal Server Security)
- Network login banners
- Login configuration RADIUS
- Login configuration TACACS

GETTING ASSISTANCE

REPORTING PROBLEMS

For a fast response, please take the time to fill out the System Problem Report to inform us of any difficulties you have with our products. A copy of this report can be found at the end of this chapter. This report provides us with important information to diagnose and respond to your questions. Please pay special attention to the following areas:

FAX Header
The System Problem Report has been designed as a FAX form. Please fill in all information in this area before you FAX the report to Cabletron Systems. If you plan to mail the System Problem Report, please fill in the company information in this section for reference information.

Software
Please fill in the following sections:
Release, Issue, and Version (From the VERsion command.)

Hardware
Select the Platform and resources that you are using.

Problem
Please fill in the following sections:
Type (Software, Hardware, Unknown.)
Occurrence (Reproducible, Intermittent, Single Occurrence.)
Original Number (This field is for your use. Enter your problem tracking number, if desired, for future reference.)
Description (Briefly describe the problem you are experiencing.)

Description (including sequence of events):
Briefly describe the problem you are experiencing. As best you can, describe the events or conditions that led to the problem you are experiencing.

Please send the System Problem Report form and any extra information (for example, line traces, system reports, and configuration files) that you have.

CONTACTING CABLETRON SYSTEMS

You can call us directly at:
Phone: (603) 332-9400
FAX: (603) 337-3075 fax

or, you can send email to us at:
support@ctron.com

You may also access our web site for further information: `http://www.cabletron.com`

DATE: _____ NUMBER OF PAGES INCLUDING THIS PAGE: _____

TO: CUSTOMER SERVICE
Cabletron Systems
(603) 332-9400 PHONE
(603) 337-3075 FAX

FROM: _____
COMPANY:_____
ADDRESS: _____
_____
PHONE: _____
FAX: _____

CABLETRON SYSTEMS
SYSTEM PROBLEM REPORT

SOFTWARE

Release: _____ Issue: _____ Version: _____

HARDWARE

Platform		Resources	
__ CSX154	__ 9W006-200	__ Ethernet-1	__ BRI-4
__ CSX155	__ 9W006-400	__ Ethernet-2	__ V.35
		__ PRI-8	__ RS232
__ CSX1200	__ 9W007-200	__ PRI- 23	__ DM8
__ CSX5500	__ 9W007-400	__ PRI- 23/30	__ DM24
__ CSX6000	__ 9W007-220	__ Expander	__ DM24+
__ CSX7000		__ BRI-1	__ DM30

PROBLEM

Type	Occurrence
__ Hardware	__ Reproducible
__ Software	__ Intermittent
__ Unknown	__ Single Occurrence

DESCRIPTION (including sequence of events prior to problem occurrence):

_____

_____

_____

_____

_____

_____

CABLETRON SYSTEMS USE ONLY

Control No:	Priority:	Date Received:
Resolution:		

ADMINISTRATIVE CONSOLE COMMANDS TABLE

The following table lists all system administration commands. Guest commands are identified in the command column.

Command	*Use*
? (GUEST)	displays help screen
atalk arp	displays the AARP cache
atalk ping <dnet>.<dnode> {timeout/dnnn] *example:* *atalk ping 1.3 30 /d200*	pings a specified device, where: dnet = destination network number (required) dnode = destination node ID (required) timeout = seconds to wait for reply (optional) nnn = data size included in ping packet (optional)
atalk port	displays AppleTalk port information
atalk port stats [clear]	displays or clears current AppleTalk port statistics
atalk route	displays AppleTalk static route information
atalk stats	displays all six groups of current AppleTalk statistics the commands below display individual group statistics
atalk stats atp	displays current AppleTalk ATP statistics
atalk stats ddp	displays current AppleTalk DDP statistics
atalk stats echo	displays current AppleTalk AEP statistics
atalk stats nbp	displays current AppleTalk NBP statistics
atalk stats rtmp	displays current AppleTalk RTMP statistics
atalk stats zip	displays current AppleTalk ZIP statistics
atalk zone	displays AppleTalk zone information
br stats	displays current packet statistics
br stats clear	clears current packet statistics
br stpbrdg	displays Spanning Tree bridge information
br stpport <port #>	displays Spanning Tree information for the specified port
call peer *<phone number> [data rate]*	calls a device at the given phone number, data rate is optional
call device <device name>	calls the specified device
cdr stats (GUEST)	displays call detail recording statistics
cdr stats clear (GUEST)	clears current call detail recording statistics

Command	*Use*
cdr verify (GUEST)	verifies call detail recording servers are configured
cfg	provides information on changes to configuration files
cfgedit	starts the CFGEDIT configuration utility
cls (GUEST)	clears administration screen
cmp stats	displays the compression connection statistics for all active connections
cmp stats <device name>	displays the compression connection statistics for the specified device
cmp clear <device name>	clears all the compression statistics for the specified device
cmp clearall	clears all active connection compression statistics
cr stats	displays the call restriction statistics
cs (GUEST)	displays connected device information
da	displays authentication messages
date <month, day, year>	changes the date as specified
dhcp stats	displays DHCP statistics
dhcp stats clear	clears DHCP statistics
disc device <device name>	disconnects all calls to the specified device
dr (GUEST)	displays message reports
ds (GUEST)	displays system statistics
ea	erases current authentication messages in memory
er	erases current system messages in memory
es	erases current system statistics in memory
exit (GUEST)	terminates a session
fr a <frame relay access "n">	sets frame relay access index to "n" as default context for all subsequent "fr" console commands
fr clear	clears the statistics counters for the selected frame relay access and DLCI
fr clearall	clears all statistics for the selected frame relay access and DLCI
fr cong	displays congestion control information for the selected frame relay access and DLCI
fr d <DLCI "m">	sets DLCI value to "m" as default DLCI for the selected frame relay access

Command	*Use*
fr dbg level	displays the current debug level for frame relay
fr dbg level <level>	sets the current debug level for frame relay
fr display	displays the configuration information for the selected frame relay access
fr lmi	displays LMI link information for the selected frame relay access
fr stats	displays statistics for the selected frame relay access and DLCI
ip addrpool	displays the current IP address pool
ip arp	displays current ARP cache table
ip filter trace <discard> <off>	controls the tracing of packets which are discarded as a result of IP filters
ip ping <host ip address>	sends an ICMP echo message to the specified host
ip rip interface	displays IP RIP interface information
ip rip routes	displays IP RIP routing table(s)
ip rip send	forces an IP RIP update message to be sent
ip rip stats	displays IP RIP statistics
ip route	displays the current routing table
ip route <IP address>	displays the routing information for the indicated device
ip stats	displays or resets current IP related statistics
ipconfig	allows you to change the system's default IP address
ipx diag <host>[timeout]	sends a diag packet to the specified host to confirm connectivity; timeout value optional
ipx ipxwan clear	clears IPXWAN stats
ipx ipxwan stats <device>	displays system-level or device-level statistics
ipx ping <host>	sends an ICMP echo message to the specified host
ipx rip stats	displays IPX RIP statistics
ipx route	displays the current IPX routing table
ipx route stats	displays IPX routing table statistics
ipx sap stats	displays IPX SAP statistics
ipx service	displays routes to IPX services
ipx service stats	displays current service table statistics

Command	*Use*
ipx sap stats	displays IPX SAP statistics
ipx spoof stats	displays IPX spoofing statistics
ipx stats	displays IPX statistics
ipx trigreq <device>	generates a triggered RIP/SAP update request to the specified device.
ipx trigrip stats	displays the triggered RIP statistics
ipx trigsap stats	displays the triggered SAP statistics
isdn usage	displays ISDN B-channel monitoring information
isdn usage clear	clears portion of ISDN B-channel monitoring information
lan stats	displays current LAN packet forwarding information
lan stats clear	clears current LAN packet forwarding information
lan test	tests for proper LAN connections
led status	allows you view snapshot of remote device's LED information
list [file name]	displays the indicated file useful for displaying Release Notes ("list rel_notes.txt")
log cdr display (GUEST)	local log file only - displays the call detail recording log report
log cdr erase (GUEST)	local log file only - erases the call detail recording log report
log cdr write (GUEST)	writes the local call detail recording log to disk
logout (GUEST)	terminates a session
manage	switches the system to the Manage Mode, allowing Dynamic Management to operate
mc (GUEST)	displays connection monitor screen
modem add <slot# modem#>	adds a modem back to available list
modem delete <slot# modem#>	deletes a modem from available list
modem reset <slot# modem #>	resets specified modems on specified slot
modem restart <slot#>	restarts the digital modem board only
modem stats <slot# modem#>	displays modem statistics for specified modem
modem stats clear <slot # modem #>	clears modem statistics for specified modem
modem status	displays slots that have valid digital modem boards

Command	*Use*
modem upgrade <slot# modem#>	installs new modem firmware onto specified modem
modem devices <data>	displays active modem connections
neif	displays the interface table
pkt capture <connection mode>	specifies which packets will be captured by the packet capture feature (all, reqd, pend, actv, idle, or none)
pkt mac	enables the MAC address monitor display
pkt [on/off]	enables or disables the Packet Capture feature
pkt display	displays captured packets
pkt load <filename>	loads previously saved Packet Capture file into memory
pkt save <filename>	saves captured packets to a disk file
primcsm	displays message indicating whether or not CSM acting as a Primary Service
pswd (GUEST)	changes password for current access level
quit	terminates system program
radius chap	attempts a RADIUS authentication session using CHAP
radius iphost	attempts a RADIUS authentication session using IP Host resolution
radius ipres	attempts a RADIUS authentication session using IP resolution
radius macres	attempts a RADIUS authentication session using MAC resolution
radius pap	attempts a RADIUS authentication session using PAP
restore	copies backup config files into current files
restart	restarts the system program remotely using Telnet
sentry ace	attempts an authentication session using ACE
sentry radius	attempts an authentication session using RADIUS
sentry status	displays current status of user level authentication servers
sentry log	logs rejection messages from the authentication server
ser <slot #> stats	displays current serial interface statistics for each V.35 or RS232 line attached to card in specified slot.
ser <slot #> clear	clears current serial interface statistics for each V.35 or RS232 line attached to card in specified slot.

Command	*Use*
ser <slot #> signal	displays current state of input signals for each serial line attached to card in specified slot. *"0"* indicates inactive; *"1"* indicates active.
session	displays the current active administration sessions
session kill <session id>	terminates the active session specified by the session id
snmp stats	displays current SNMP related statistics
sp	lists each semi-permanent device and associated status
start_ne	starts or restarts system software
status (GUEST)	displays system errors and system messages
tcp conns	displays the current TCP connection status
tcp stats	displays the current system TCP statistics
telnet	puts you in the Telnet command mode see `telnet mode commands` for available commands
telnet <ip-address>[port #]	begins a Telnet session for the indicated Telnet host
telnet mode commands: *close* *exit* *open [target host][port #]* *send [send parameter]* *set <name><value>* *status* *toggle*	 closes the current Telnet connection to a target host closes the current Telnet session establishes a Telnet session with a target host sends special Telnet control functions to the currently connected target host sets operating parameters for the current Telnet session provides information about the current Telnet session sets operating parameters for the current Telnet session
term	displays the terminal type.
term set <terminal type>	sets the terminal type
tftp get	invokes the TFTP GET command
tftp put	invokes the TFTP PUT command
tftp session	displays TFTP session statistics
tftp session kill <session id>	terminates the active TFTP session specified by the session id
tftp stats (GUEST)	displays the current TFTP statistics
time[hours:minutes:seconds]	displays or changes current system time
trace [on/off]	enabled or disables call trace information reports
trace ipxwan [on/off]	enables or disables the IPXWAN tracing option

Command	*Use*
trace lapb[on/off]	enables or disables the packet tracing option for LAPB data link information
trace ppp [on/off]	enables or disables the tracing of ppp packets
trace x25 [on/off]	enables or disables the packet tracing option for X.25 connection information
udp conns	displays UDP connection status
udp stats	displays UDP statistics
ver (GUEST)	displays current software version and hardware resource revision information
wa	writes current authentication messages to disk
wan fr-ietf stats [device/ fr_accessname_dlci] [prot]	displays WAN frame relay connection information for devices configured for the FR_IETF line protocol
wan fr-ietf trace [on/off] [in/out] [device/fr_accessname_dlci] [prot]	enables or disables the tracing for WAN FR_IETF packets
wan stats	displays current WAN connection information
wr	writes current system messages to disk
ws	writes current system statistics to disk
x25 clear	clears the statistics counters for the currently selected X.25 access
x25 clearall	clears all statistics for the currently selected X.25 access
x25 display [access name] (GUEST)	displays the configuration information for the default X.25 access or the specified access
x25 l <LCN "m"> (GUEST)	sets LCN index default value to "m"
x25p<accessname>(GUEST)	sets X.25 access name default to the specified access name
x25 stats [l <access name>] (GUEST)	displays statistics for the default X.25 access or for the specified X.25 access
x25 vc <LCN "m">	sets the LCN index default value to "m", which will specify the default virtual circuit
x25 vc active	lists all active virtual circuits
x25 vc clear	clears statistics for a virtual circuit
x25 vc stats	displays statistics for a virtual circuit

MANAGE MODE COMMANDS TABLE

The following table displays the available Dynamic Management commands:

Command	*Use*
ace	displays ACE off-node server configuration
ace change	allows changes to the ACE off-node server configuration
ace reinit	reinitializes the CyberSWITCH ACE client
admlogin [change]	displays [or allows you to change] the current administrative session configuration information
alarm	displays the current enabled status of the call restriction alarm
alarm [off/on]	disables / enables the audible call restriction alarm
bwres	displays the current state of the bandwidth reservation feature
bwres [on/off]	allows you to enable / disable bandwidth reservation
callrest	displays the current call restriction configuration data
callrest [off/on]	disables / enables the call restriction feature
cls	clears the display screen
commit	writes the current system data to the configuration file
commit status	displays the Manage Mode updates made since configuration data was last committed
csm	displays current CSM configuration data
csm change	allows you to change the CSM TCP port number
datalink	displays the current data link configuration data
datalink [add/change/delete]	adds / changes / deletes a data link
dedacc	displays the current dedicated access configuration data
destfilt	displays the current destination address filter configuration data
destfilt [add/change/delete]	adds / changes / deletes a destination address filter
device	displays the current on-node device table
device [add/change/delete]	adds / changes / deletes a on-node device entry
dhcp	displays current DHCP configuration data
dhcp change	changes current DHCP data

Command	*Use*
exit	exits from Manage Mode and returns to the normal system command mode
fileattr	displays the current user file access rights (guest or admin)
fileattr change	allows you to change current file access rights configuration data
help	displays a list of the valid Manage Mode commands
ipfilt	updates the IP filter configuration
ipnamesv	configures DNS and NetBIOS name server addresses
ipnetif	displays the current IP network interface configuration data
ipradius	displays current enabled status of IP route lookup via RADIUS
ipradius off	disables lookup of IP routes via RADIUS
ipradius on	enables lookup of IP routes via RADIUS
iprip	displays selected type of RIP information
iprip [off/on]	disables / enables RIP
iproute	displays the current IP static route configuration data
iproute [add/change/delete]	adds / changes / deletes an IP static route
ipxaddrpool	displays current IPX address pool
ipxaddrpool [add/change/delete]	adds / changes / deletes an IPX address from the IPX address pool
ipxinet	allows you to enter the network number for the IPX router
ipxiso	allows you to enable / disable IPX isolated mode
ipxnetif	displays current IPX network interface data
ipxnetif [add/change/delete]	adds / changes / deletes an IPX network interface
ipxrip	displays the current IPX RIP status (enabled or disabled)
ipxrip [off/on]	disables / enables IPX RIP
ipxroute	displays current IPX routes
ipxroute [add/change/delete]	adds / changes / deletes an IPX route
ipxsap	displays the current IPX SAP status (enabled or disabled)
ipxsap [off/on]	disables / enables IPX SAP
ipxsvc	displays current IPX service data

Command	*Use*
ipxsvc [add/change/delete]	adds / changes / deletes an IPX service
ipxspoof	allows you to configure system level spoofing data
ipxt20	allows you to configure IPX type 20 information
line	displays the current line configuration data
lineprot	displays the current default line protocol configuration
lineprot change	allows changes to default line protocol configuration
log	presents all configuration options for log options
netlogin	displays network login parameters
netlogin change	allows changes to the network login parameters
offnode	allows changes to current settings for off-node server options, including Radius accounting, RFC2138, and dynamic device options
options	displays the current operating mode, security options, and system parameters
options change	allows the current system parameters to be changed
pktfilt	displays the current packet filter configuration data
pktfilt [add/change/delete]	adds / changes / deletes a packet filter
profile	displays current profile table
protdef	displays the current protocol definition configuration data
protdef [add/change/delete]	adds / changes / deletes a protocol definition
protfilt	displays the current protocol filter configuration data
protfilt [add/change/delete]	adds / changes / deletes a protocol filter
radius	displays RADIUS off-node server configuration
radius change	allows changes to the RADIUS off-node server configuration
readme	displays helpful tips on how to use the Manage Mode commands
resource	displays the current resource configuration data
seclevel	displays current security level
semiperm	allows you to add or delete device entries for semipermanent connections
snmp	displays the current SNMP configuration data

Command	*Use*
srcfilt [add/change/delete]	adds / changes / deletes the a source address filter
tacacs	displays TACACS off-node server configuration
tacacs change	allows changes to the TACACS off-node server configuration
termopt	allows you to change default async protocol configuration
tftp	displays the current TFTP configuration
tftp change	allows the current TFTP configuration to be changed
thruput	displays the current throughput monitor configuration data
thruput change	allows the current throughput monitor configuration data to be changed

CAUSE CODES TABLE

The following table provides Q.931 cause codes and their corresponding meanings. Cause codes may appear in Call Trace Messages.

Dec Value	*Hex Value*	*Q.931 Cause*
0	0	valid cause code not yet received
1	1	unallocated (unassigned number) Indicates that, although the ISDN number was presented in a valid format, it is not currently assigned to any destination equipment.
2	2	no route to specified transit network (WAN) Indicates that the ISDN exchange was asked to route the call through an intermediate network that is unrecognized.
3	3	no route to destination Indicates that the call was actually routed through a network that does not serve the destination address.
4	4	send special information tone
5	5	misdialed trunk prefix
6	6	channel unacceptable Indicates that the quality of service provided by the specified channel was insufficient to accept the connection.
7	7	call awarded and being delivered in an established channel Indicates that the device has been awarded an incoming call and that the call is being connected to a channel that has already been established for similar calls.
8	8	prefix 0 dialed but not allowed
9	9	prefix 1 dialed but not allowed
10	A	prefix 1 dialed but not required
11	B	more digits received than allowed, call is proceeding
16	10	normal call clearing or normal disconnect Reports the normal clearing of a call. No action required.
17	11	device busy Indicates that the called system has acknowledged the connection request, but is unable to accept the call because the B-channels are currently in use.
18	12	no device responding Indicates that the connection could not be completed because the destination failed to respond to the call.

Dec Value	*Hex Value*	*Q.931 Cause*
19	13	no answer from device (device alerted) Indicates that the destination has responded to the connection request but has failed to complete the connection within the prescribed time. Problem at remote end.
21	15	call rejected Indicates that the destination was capable of accepting the call (was neither busy nor incompatible) but rejected the call for some reason.
22	16	number changed Indicates that the ISDN number used to set up the call is no longer assigned to any system. If an alternate address has been assigned to the called equipment, this may be returned in the diagnostic field of this message.
23	17	reverse charging rejected
24	18	call suspended
25	19	call resumed
26	1A	non-selected device clearing Indicates that the destination was capable of accepting the call (was neither busy nor incompatible) but rejected the call because it was not awarded to the device.
27	1B	destination out of order Indicates that the destination could not be reached because the interface was not functioning correctly and a signaling message could not be delivered for some reason. This may be a temporary fault but one that is expected to last a relatively long time. For example, equipment off-line.
28	1C	invalid number format (incomplete number) Indicates that the connection could not be established because the destination address was presented in an unrecognized format or because the destination address was incomplete.
29	1D	facility rejected Indicates that the facility requested by the device could not be provided by the network. This could be a subscription problem.
30	1E	response to STATUS INQUIRY Indicates that the status message was generated in direct response to the prior receipt of a status enquire message.
31	1F	normal, unspecified Reports the occurrence of a normal event when no standard cause applies. No action required.
33	21	circuit out of order

Dec Value	*Hex Value*	*Q.931 Cause*
34	22	no circuit / channel available Indicates that the connection could not be established because there was no appropriate channel available to handle the call.
35	23	destination unattainable
37	25	degraded service
38	26	network (WAN) out of order Indicates that the destination could not be reached because the network was not functioning correctly and that the condition is expected to last for a relatively long time. An immediate re-connect attempt is likely to be unsuccessful.
39	27	transit delay range cannot be achieved
40	28	throughput range cannot be achieved
41	29	temporary failure Indicates that an error has occurred because the network is not functioning correctly, but that this problem is likely to be resolved shortly.
42	2A	switching equipment congestion (network congestion) Indicates that the destination could not be reached because the network switching equipment was temporarily overloaded.
43	2B	access information discarded Indicates that the network could not provide the requested access information.
44	2C	requested circuit / channel not available Indicates that the remote equipment could not provide the requested channel for an unspecified reason. This may, or may not, be a temporary problem.
45	2D	preempted
46	2E	precedence call blocked
47	2F	resource unavailable, unspecified Indicates that the requested channel or service was unavailable for an unspecified reason. This may, or may not, be a temporary problem.
49	31	quality of service unavailable Indicates that the requested quality of service (as defined by CCITT recommendation X.213) could not be provided by the network. This may be a subscription problem.
50	32	requested facility not subscribed Indicates that the remote equipment supports the requested supplementary service but that this is available only by subscription.
51	33	reverse charging not allowed

Dec Value	*Hex Value*	*Q.931 Cause*
52	34	outgoing calls barred
53	35	outgoing calls barred within CUG
54	36	incoming calls barred
55	37	incoming calls barred within CUG
56	38	call waiting not subscribed
57	39	bearer capability not authorized Indicates that the device has requested a bearer capability that the network is able to provide, but that the device is not authorized to use. This may be a subscription fault.
58	3A	bearer capability not presently available Indicates that the network is normally able to provide the requested bearer capability, but not at the present time. This may be a temporary network problem or a subscription problem.
59	3B	device busy 1TR6
61	3E	call rejected 1TR6
63	3F	service or option not available, unspecified Indicates that the network or remote equipment was unable to provide the requested service option for an unspecified reason. This may be a subscription problem.
65	41	bearer service (or capability) not implemented Indicates that the network is not capable of providing the bearer capability requested by the device.
66	42	channel type not implemented Indicates that the network or the destination equipment does not support the requested channel type.
67	43	transit network selection not implemented
68	44	message not implemented
69	45	requested facility not implemented Indicates that the remote equipment does not support the requested supplementary service.
70	46	only restricted digital information bearer capability is available Indicates that the network is unable to provide *unrestricted* digital information bearer capability.
79	4F	service or option not implemented, unspecified Indicates that the network or remote equipment was unable to provide the requested service option for an unspecified reason. This may be a subscription problem.

Dec Value	*Hex Value*	*Q.931 Cause*
81	51	invalid call reference value Indicates that the remote equipment has received a call with a call reference that is not currently in use by the device-network interface.
82	52	identified channel does not exist Indicates that the receiving equipment has been requested to use a channel that is not activated on the interface for calls.
83	53	a suspended call exists, but this call identity does not Indicates that the network received a call resume request. The call resume request contained a Call Identity information element which indicated that it is in use for a suspended call.
84	54	call identity in use
85	55	no call suspended Indicates that the network received a call resume request when there was not a suspended call pending. This may be a transient error that will be resolved by successive retries.
86	56	call having the requested call identity has been cleared Indicates that the network received a call resume request. The call resume request contained a Call Identity information element which once indicated a suspended call; however, that suspended call was cleared either by time-out or by the remote device.
88	58	incompatible destination Indicates that an attempt was made to connect to non-ISDN equipment; for example, to an analog line.
89	59	non-existent abbreviated address entry
90	5A	remote device initiated 1 TR6
91	5B	invalid transit network specified Indicates that the ISDN exchange was asked to route the call through an intermediate network that is unrecognized.
92	5C	invalid facility parameter
93	5D	mandatory information element is missing
95	5F	invalid message unspecified Indicates that an invalid message was received and that no standard cause applies. D-channel error. If this error is returned systematically, report the occurrence to your authorized service provider.
96	60	mandatory information element is missing Indicates that the receiving equipment received a message that did not include one of the mandatory information elements. D-channel error. If this error is returned systematically, report the occurrence to your authorized service provider.

Dec Value	*Hex Value*	*Q.931 Cause*
97	61	message type non-existent or not implemented Indicates that the receiving equipment received a message that was not recognized either because the message type was invalid, or because the message type was valid but not supported. This is either a problem with the remote configuration or a problem with the local D-channel.
98	62	message not compatible with call state or message type non-existent or not implemented or wrong message Indicates that an invalid message was received and that no standard cause applies. D-channel error. If this error is returned systematically, report the occurrence to your authorized service provider.
99	63	information element nonexistent or not implement Indicates that an invalid message was received by the remote equipment that contained information elements which were not recognized. D-channel error. If this error is returned systematically, report the occurrence to your authorized service provider.
100	64	invalid information element contents Indicates that a message was received by the remote equipment that included invalid information in the information element. D-channel error.
101	65	wrong message for state (message not compatible with call state) Indicates that remote equipment received an unexpected message that did not correspond to the current state of the connection. D-channel error.
102	66	recovery on timer expiry Indicates that an error-handling (recovery) procedure has been initiated by a timer expiry. This should be a temporary problem.
103	67	mandatory information element error
111	6F	protocol error Indicates an unspecified D-channel error when no other standard cause applies.
112	70	local procedure error 1TR6
113	71	remote procedure error 1TR6
127	7F	internetworking, unspecified Indicates that an event occurred but that the network does not provide causes for the actions that it takes, therefore the precise nature of the event cannot be ascertained. This may, or may not, indicate the occurrence of an error.

Dec Value	*Hex Value*	*Q.931 Cause*
UNKNOWN		Indicates that an event occurrent but that the network does not provide causes for the actions that it takes, therefore the precise nature of the event cannot be ascertained. This may, or may not, indicate the occurrence of an error.

INDEX

A

access request retries 219, 221
accesses
  alternate accesses 242, 429
  dedicated 242
  frame relay 255
  ISDN access 242
  X.25 244
accessing the CyberSWITCH 98
ace 221
ACE Authentication Server
  alternate method of configuring 221
  configuring 220
action on data timeout 393
active WAN peer 348
adapter switch settings 86
adapters 58
  basic rate 59, 670
  cabling 94
  configuring adapters 115
  DM-24 68, 678
  DM-8 68, 677
  Ethernet 58, 669
  overview 117
  PRI-23 61, 672
  PRI-23/30 62, 673
  PRI-8 61, 671
  primary rate adapters 61, 671
  RS232 65, 676
  slot selection 84
  V.35 64, 675
admin 103, 576
admin login names 103
administration console
  commands 701
  connecting 98
  requirements 84
administration software 70
air filter
  cleaning the CSX5500 air filter 43
  cleaning the CSX6000 air filter 47
  cleaning the NE 5000 air filter 56
alarm 373
AMI encoding 125
AppleTalk routing 357
  capacities 363
  commands 587
  configuring 357, 358, 359, 363, 364
  device information 189
  port statistics 633
  remote LAN 361
  static routes 362
  statistics 629
  verification 452
  verifying initialization 452
  verifying over LAN 453
  verifying over WAN 455
asynchronous connections
  AUD 391
  authentication 395
  default async protocol 392, 394
  PPP mode configuration 392
  terminal mode configuration 393
asynchronous usage discriminator 118, 391
ASYNDMPORT 119
atalk 357
atalk commands 587
atalk port stats 633
atalk stats 629
AUD 118, 391
authentication 188
authentication databases 162
authentication header 231
authentication header (AH) 232
automatic TEI negotiation 122
autosense 33, 395

B

B8ZS encoding 125
backup
  diskette 84
  redundant configurations 150
bandwidth 31
  bandwidth reservation 376, 379, 463
  limitations 192
banners 225
base data rate 192
basic rate adapters 59, 670
basic rate ISDN lines
  auto TEI 122
  line interface type 122
basic rate_net 115
B-channel 607
br stat 592
br stp commands 614
BRI initialization message 420

bridging
bridge password 195
configuration 268
dial out 264
device list configuration 265
using bridge filters 283
using known connect list 285
filters 269
operation verification 423
overview 268
problem diagnosis (initialization) 462
statistics 634
bus cable 95

C

cabling
adapters 94
for multiple WAN adapters 95
requirements 83
call commands 592
call control 365
call detail recording 404, 405, 634
viewing reports 404
call interval parameters 371
call restrictions
configuring 372, 373
statistics 628
call screening methods 119, 122
call statistics 628
call trace messages 545, 712
callback 385
callrest 373
Carbon Copy 70, 99, 100, 101, 570
cause codes table 712
CDR
commands 596
operation verification 461
viewing reports 404
cdr 392
CDR. Also see *call detail recording* and *log options*.
cfg 585
CFGEDIT 111, 665
cfgedit command 112
map 691
CHAP secret 194, 217
CLID 195, 386
clocking 116
cls 113, 578
cmp commands 597
commands
administration services 576
AppleTalk 587
bridging 591
call control 592
call detail recording 596
call restriction 596
compression 597
CSM 597
digital modem 598
dynamic management 708
frame relay 599
IP routing 601
IPX 605
ISDN usage 607
LAN 608
log 608
operational information 578
packet capture 609
RADIUS 612
security (user-level) 623
set date and time 586
SNMP 614
spanning tree 614
summary 701, 708
TCP 617
Telnet 618
terminal 620
terminating and restarting 585, 586
TFTP 621
throughput 582
trace 622
UDP 623
WAN 624
X25 625
commit 113
committed information rate 259
common channel 125
COMMPORT 33, 118, 121, 126
community name 352
compliance notices 3
compression 31, 410
and CCP 412
configuration elements 199
configuring 410
operation verification 462
PPP compression and encryption 240
problem diagnosis 462
statistics 635

configuration
files 71, 665
packet types 292
restoring 666
tools
CFGEDIT 111
dynamic management 112
congestion control 259
connection filters 297, 303
Connection Services Manager. *See CSM*.
connections table 581
connectivity statistics 627
console connections
digital modem 102
direct 98
null-modem 99
remote 101
remote analog console access 391
using telnet 100
Console Information Port (CIP), refers to RS232 port
country code 117
CPE 117, 124
cr stats 596
crossover cable 95
cs 392, 578
CSM 34, 37, 208, 383, 385
commands 597
CSU 61, 63, 80, 125
CSX5500 42
CSX6000 46
CSX7000 49
custom information 666

D

D channel callback 385
D Channel callback verification 469
da 72, 578
da 404, 480
data line idle character 126
data links 122
data timeout value 394
database timer (triggered RIP/SAP) 343
datalink 121
date 586
DC powered platforms 45, 48, 50
decompression statistics 635
dedacc 242
dedicated access 242
configuration 243
device authentication 243
line protocol 242
dedicated connections 148
default line protocol 399
default per-device 411
default profile 377
default routes 157
DES 32, 89, 231, 682
destfilt 271
destination IP address 154
destination MAC filter commands 271
device 191, 347
device level databases 183
device level security 161, 167
device profile 376, 378
DHCP
commands 597
example configurations 311
in a bridge to bridge environment 310
in a router to bridge environment 310
proxy client 315
proxy client verification 467
relay agent 308
relay agent verification 464
statistics 636
verifying 464
dhcp 308, 315
dhcp commands 597
diagnosing problems 417
dial out 32, 196
number 193
using bridge filters 283
verification 459
digital modem 32, 67, 389
adapter settings 86, 87, 88
background information 118, 390
configuring 389
device information 187
inactivity timeout 387, 388
MVIP termination 89
remote site requirements 390
directory number 124
disc device 595
DLCI value 258
DM-24+ 68, 680
DM-30+ 68, 680
DM-8, DM-24, DM-30. See digital modem.
DMS100 78, 123
DNS 319, 320
DOC notice 4
dr 72, 578
dr 404, 480
ds 72, 578, 627
DSU 64

dynamic device option 216
dynamic management 577
    command summary 708

E
E1/R2 signaling 127
EMS 49
Encapsulating Security Payload (ESP) 33
encapsulation 136, 327
encryption 32, 160, 236
    configuration 231
    link layer 238
    network level 236
encryption adapters 69, 89, 231, 682
encryption method (ACE) 222
er 584
error messages 481
error threshold count 258
es 584
ESP Tunnel mode 33, 36, 239
Ethernet adapters 58, 669
exception filter 298, 303
excess information rate 259
exit 577
external network number 325
EZ-ISDN codes 75

F
FCC notice 3
features 31
file attributes 415
fileattr 415
filters 31
    See also bridging, dialout, IP filters
final condition 299
flattening (network) 150
forwarding filters 296, 302
fr commands 599
frame relay
    congestion control 262
    data rate control 261
    local management interface 261
    max number of accesses 255
    operation verification 430
framing types 120, 124

G
Gateway/Router IP Address 235
generic number 117
global timers 342
guest 576

H
H0 call support 185, 193
hardware
    adapters 58, 668
    installation 83
    overview 41
    platforms 41
    verification 418
HDLC bridge devices 199
HDLC data polarity 257
help 113, 578
hold-down timer (triggered RIP/SAP) 343
hunt group 80

I
ICMP 295
ICMP group statistics 645
idle condition 369, 392
initial data rate 192
initialization messages 481
initiating a connection 100
install 105
installation
    inserting adapters 93
    requirements 83
    slot selection 84
    switch settings 85
interfaces 130, 133
    LAN 133
    WAN 134
    WAN direct host 134
    WAN IP UnNumbered 135
    WAN RLAN 134
internal network number 325
IP addresses 133, 135, 577
    IP filters 300
    multiple (also see secondary IP addressing) 240
ip addrpool 598
ip commands 601
IP encryption 236
IP filters 291, 301
    applying filters 299
    configuration elements 300
    connection filters 297
    encryption 239
    example 306
    exception filter 298
    forwarding filters 296
    global 299
    ICMP configuration 295
    network interfaces 299

IP filters, continued
packet type configuration 292
per-device 299
TCP configuration 294
trace messages 551
UDP configuration 294
verification 440
IP host devices 201
IP host mode
host identifier 195
interface 132, 135
verifying 427
IP operating mode 131
ip rip commands 602
ip route commands 604
IP routing
address pool 290
commands 601
configuring 130
enabling 130
isolated mode 289
network interfaces 133
operation verification 423
over LAN interface connection
problem diagnosis 434
verification 433
over WAN interface connection
problem diagnosis 436
verification 434
over WAN remote interface connection
verification 438
over WAN unnumbered interface connection
verification 439
static ARP table entries 288
static route lookup via RADIUS 289
statistics 643
verifying interfaces 433
ipconfig 577
IPCP
address negotiation initiation 397
ipfilt 292
ipnamesv 320
ipnetif 135
ipradius 289
iprip 159
iproute 153
ipx commands 605
ipx route stats 649
IPX routing 321
background information 324
commands 606
configuring devices 265, 344
device IPX configuration elements 347
enable RIP/SAP 330
Frame Relay 189, 345, 349
internal network number 324
IPX RIP and SAP processing options 330
LAN port number 327
network interface 325
network number 327
protocols 348
remote LAN interface 329, 332
RIP table size 330
routing tables 331, 451
SAP table size 330
service tables 331, 451
statistics 646
triggered RIP/SAP 342
verification 446
verifying over LAN 447
verifying over remote LAN 448
verifying over WAN 450
verifying triggered RIP/SAP 450
WAN interface 329
IPX WAN
protocol 348
ipxinet 324
ipxiso 341
ipxnetif 326
ipxrip 330
ipxroute 334
ipxsap 330
ipxsvc 335
ipxt20 340
ISDN
configuration elements 191
ordering 75
profile information 378
provisioning settings 75
isdn usage commands 607
isolated mode 289

J

jumper settings 86

K

known connect list 285

L

LAN adapter
  initialization messages 419
  problem diagnosis 423
  verification messages 422, 423
lan commands 608
LAN IP interface 133
LAN statistics 642
lan test 422
LAPB 248
LCD cables 96
LCD messages 475
line 121
line build out 125
line encoding 125
lineprot 400
lines 119
  background information 126
  call screening methods 122
  configuration 119, 122
  for BRI resource 119
  for PRI resource 119
  line interface type 122
  line type 126
link failure detection 257, 397
link layer encryption 231, 238
list (file name) 578
LMI 261
  format 258
  overview 261
local user list
  Now referred to as on-node device database 183
log cdr commands 608
log options 400
  call detail recording events 406
  CDR log report 405
  configuration elements 401
  local log file 402
  syslog server 402
log options 401
login 103, 106
login commands 576
logout 577

M

maintenance 665
make calls option 196, 347
manage 113, 577
Manage Mode 111, 113, 577, 666, 708
maximum data rate 192
maximum retransmissions 343
mc 392, 579, 582
messages
  authentication messages 404
  CDR 404
  LCD messages 475
  system messages 404, 480
  trace messages 544
metric value 153, 154, 157
MIBs
  access level 352
  enterprise 355
  enterprise MIBs for Spectrum 356
  MIB-2 354
modem 67
modem callback 385
modem callback verification 470
modem commands 598
modem devices 599
modem inactivity timeout 387, 388
modinact 387
monitored events count 258
monthly call charge 371
MTU 136, 327
multi-level security
  operation verification 426
  user defined 188
multiple admin login names 103
multiple IP addresses 150
multiple login admin names 207
MVIP 94
  bus connections 95
  settings 89

N

NBNS 320
NE 2000-II 51
NE 4000 53
NE 5000 55
neif 579
NET3 116
NET5 385
NetBIOS 319, 320
netlogin 224, 225, 227, 229
netstat -r 443
network flattening
  Proxy ARP 150
  secondary IP addressing 151
network login information 223
  banners 225
  specific to RADIUS 226
  specific to TACACS 228
  terminal server security 224

network number 327
network security
configuring device and user level security 172
configuring device level security 167
configuring no security 166
configuring user level security 168
network service provider
CyberSWITCH as NSP 320
network topology worksheet 684
next hop 153, 154, 157, 235
NI-1 123
NI1 385
normal operation messages 481
NSP 320

O

offnode 213, 216, 217
off-node server information 207
on-node device table: configuration elements 191
operational files 72
outbound authentication 195, 217, 386
overload condition 368
over-subscription timer (triggered RIP/SAP) 343

P

packet data filter commands 271
packet types 292, 302, 304
PAP password 194, 217
passive WAN peer 348
PCM encoding 117
ping 435
pkt commands 609
pkt mac 591
pktfilt 271
platforms 41
DC powered 45, 48, 50
point-multipoint 122
point-to-point 122
polling timer (triggered RIP/SAP) 343
port statistics, AppleTalk 633
power requirements 83
powering on 98, 99
PPP
bridging 202
configuring 396
link failure detection 398, 430
reference documents 399
routing 201
STAC-LZS
extended mode 413
sequence number 199, 413
verify link detection failure 430
PPP mode (async) 392
PPP packet trace messages 552
prefetching IP addresses 316
PRI adapters
PRI connection 63
PRI-23 91
PRI-23/30 settings 92
PRI-8 settings 90
PRI-23 adapter 61, 672
PRI-23/30 adapter 62, 673
PRI-8 adapter 61, 671
primary rate ISDN lines
framing types 124
generic number 117
line build out 125
line encoding 125
signaling method 125
synchronization type 117
primary service 597
primcsm 597
problem diagnosis 417
CDR 461
compression 462
DHCP 466
dial out 460
IP routing 434
LAN 423
SNMP 457
profile 378
profile name 185
protdef 270
protfilt 271
protocol definition commands 270
protocol definitions 273
protocol filter commands 271
proxy ARP 136, 150
verification 472
pswd 103, 577
PVCs 247, 252, 256
configuration elements 258

Q

quit 108, 585

R

R2 signaling 92, 124, 127
radacc 214
radius 211, 214
RADIUS Accounting 214
diagnosis 215
verification 215
radius commands 612

RADIUS Server
configuring 211, 214
configuring a RADIUS Accounting Server 212
configuring login information 226
configuring user-level security 205
digital modem 392
RFC2138 215
static route lookup 289
rate measurement interval 259
readme 113
region 117
regulatory compliance of platforms 44, 48, 52, 54, 57
release notes 27
remote device connectivity
operation verification 424
remote IP address 235
remote LAN 142, 325, 329, 346
remote management 560
Carbon Copy 570
remote analog console access 391
SNMP 561
Telnet 563
TFTP 568
Win95 dial-up networking 566
report log 480, 544
reporting problems 699
reports 400
resource 116
resources 115, 117, 118
See also adapters
restart 585
restore 585
restoring configuration 666
restricted bridge mode 269, 278
retransmission timer (triggered RIP/SAP) 343
RFC2138 215
RIP (IP) 158
and dedicated connections 148
and interfaces 145
commands 602
enabling 130, 158
host routes propagation scheme 140
propagation control 154, 155, 158
receive control 139
respond control 138
send control 138
v2 authentication control 139
v2 authentication key 140
verifying initialization 441
verifying LAN input processing 443
verifying LAN output processing 442
RIP (IP), continued
verifying WAN input processing 445
verifying WAN output processing 444
RIP (IPX)
description 331
entry aging time 328
network interface configuration elements 327
number of table entries 331
processing option 330
RJ-45 connector (BRI)
pin and signal assignment 60
RJ-45 connector (PRI)
pin and signal assignment 63
RLAN interface (remote LAN) 134
robbed bit signaling 125
jumper 92
routing tables (IPX) 331, 451
RS232 adapters 65, 676
pin and signal assignments 66
RS232 connection 66
RSA/DES 682
rupgrade.bat 109

S

SAP (IPX)
description 331
entry aging time 328
network interface configuration elements 328
propagation 336
seclevel 166, 167, 168, 172, 205
secondary IP addressing 134, 150, 151
Secure Wide Area Network 36, 37
SecurID card 161, 169
security
authentication databases 162
authentication process 168
device level databases 183
network login information 223
off-node server information 207
overview 161
token card 169
user level databases 205
security associations 231, 232
security level 164
device and user level security 172
device level security 167
no security 166
user level security 168
Security Parameter Index (SPI) 236
semiperm 380

semipermanent connections 379, 381
and call device commands 381
and call restrictions 382
and throughput monitor 382
commands 580
configuring 379, 381
verification 471
sentry commands 624
ser commands 614
service tables (IPX) 451
session 586
shared secret (RADIUS) 211
Shared Secret Key 235
signaling method 125
SNMP 350, 353, 561
configuring 350
remote management 561
statistics 652
verification 457
snmp 352
snmp stats 614
socket number 336
software
configuration files 71
installing 105
local upgrade 107
operational files 72
overview 70
remote upgrade 108
system files 71
upgrading 107
source MAC filter commands 270
sp 580
Spanning Tree
bridge information 615
configuration 266
messages 481
port information 614
SPID 123
srcfilt 270
start_ne 585
static ARP table entries 288
static route lookup via RADIUS 289
static routes 130
AppleTalk routing 362
configuring 152
IPX 333
statistics
AppleTalk routing 629
bridging 634
call detail recording 634
call restriction 628
statistics, continued
call statistics 628
compression 635
connectivity 627
DHCP 636
IP 643
IPX 646
IPX route 649
LAN 642
serial interface 652
SNMP 652
TCP 655
TFTP 656
throughput monitoring 628
triggered RIP/SAP 649, 650
UDP 658
WAN 658
writing to disk 72
status 581
subaddress 119, 127, 193
subnet mask 136, 153, 154, 233, 235
SVCs 254
switches 40, 116
synchronization type 116, 117
sysContact 353
sysLocation 353
sysName 353
system details worksheet 685
system files 71
system messages
error messages 481
informational messages 481
initialization messages 481
normal operation messages 481
off-node reports 404
operational files 72
Spanning Tree messages 481
summary 482
warning messages 481
writing to disk 72
system options and information 174
system report log 480, 544
system software 70

T

table size, IPX RIP and IPX SAP 330
TACACS
configuring login informaiton 228
tacacs 219
TACACS Authentication Server 218
configuration elements 219
packet format 219

TCP 294, 300, 305
statistics 655
tcp commands 617
TDM 94, 124
bus connections 95
Teleos Simulator 116
Telnet 100, 563
remote management 563
telnet commands 618
term commands 621
term set 424
terminal mode 33, 102, 392, 393, 394
authentication 395
CDR information 406
limitations 395
terminal server menu
problem diagnosis 432
terminal server security 224, 394
termopt 392
TFTP 414, 568
configuration elements 414
remote management 568
statistics 656
tftp 414
tftp commands 621
The Local IP Address 235
throughput monitor 366
configuring 366, 367
example 369
idle condition 369
overload condition 368
statistics 628
underload condition 369
thruput 366
time 581, 586
tools
for remote management 560
trace commands 623
trace lapb 625
trace messages 544
call trace messages 545
frame relay 557
IP filters 551
PPP packet 552
summary 546
WAN FR_IETF 554
X.25 554
transmit broadcast address 136
triggered RIP/SAP 342
commands 607
description 343
device information 349
global timers 342, 344
statistics 649, 650
verification 450

U

UDP 294, 300, 305
port number 219, 221
statistics 658
udp commands 623
underload condition 369
unrestricted bridge mode 268
upgrade.osw 109
upgrading software 107, 665
warnings and errors 108
user level authentication 195
user level databases 205
user level security 161, 168
configuration 168, 206
configuration specific to IPX 344, 346
device and user level security 172
login banner files 73
utility commands 113

V

V.35 adapters 64, 675
pin and signal assignments 65
V.35 connection 64
VCCI notice 4
ver 581
verification
D Channel callback 469
modem callback 470
verification and diagnosis 417
base system 418
requirements 417
routing protocols 433
system options 457
verifying the installation
AppleTalk 452
bridge initialized 423
CDR 461
compression 462
dedicated connection 429
DHCP 464, 467
dial out 459
frame relay 430
hardware resources 418
IP filters 440

verifying the installation, continued
IP host mode 427
IP router initialized 423
IP routing over interfaces 433
IPX routing 446
LAN 422
multi-level security 426
PPP link detection failure 430
proxy ARP 472
remote device connectivity 424
reserved bandwidth 463
RIP 441
semipermanent connections 471
SNMP 457
triggered RIP/SAP 450
verifying an X.25 connection 431
WAN direct host 436
WAN lines 420
virtual circuits 193, 253
vra 208

W

wa 72
WAN
direct host interface 134, 436
IP interface 134, 434
IP UnNumbered interface 135
line verification 420
remote LAN interface 438
statistics 658
wan 624
WAN (Mac Dial In) 359
WAN adapter
initialization messages 418
WAN peer type 348
wan stats 582
warning messages 481
WIN95 dial-up networking 566
worksheets 683
wr 72, 584
ws 72, 584

X

X.121 address 194, 247
X.25
access 244
charging related facilities 246
LAPB 248
LAPB messages 557
LAPB trace messages 557
miscellaneous facilities 252
operation verification 431
PVCs 247
quality of service facilities 246, 250
reliability, windows, and acknowledgment 250
restriction facilities 252
statistics 661
SVC 254
timers 245
trace messages 554
x25 commands 626